(1)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-085059
(43)Date of publication of application : 20.03.2003

(51)Int.Cl. G06F 13/00
G06F 15/00
H04L 12/46
H04L 12/66

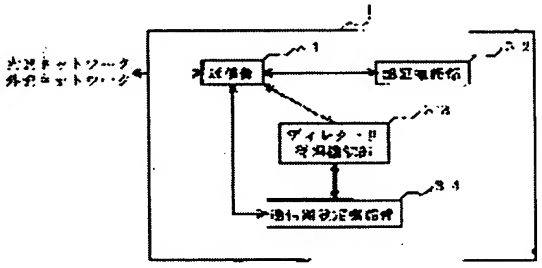
(21)Application number : 2002-068762
(22)Date of filing : 13.03.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : KOKADO TAKESHI
OKADA YASUNORI
KUBOTA KOJI
SAITO TAKAHIRO
ISHIKAWA HIROKAZU

(30)Priority
Priority number : 2001076507 Priority date : 16.03.2001 Priority country : JP
2001199977 29.06.2001 JP

(54) FIREWALL SETTING METHOD AND SYSTEM FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a firewall setting method and a system therefor that limit users having access from an external network for each terminal of an internal network and allow the users to connect to a terminal of the internal network selectively.
SOLUTION: An HGW 1 has a communication part 31, an authentication function part 32, a directory management function part 33 and a channel setting function part 34. The communication part 31 receives data communication to the HGW 1. The authentication function part 32 determines whether the data are from an authentic user or not. The directory management function part 33 receives a service registration, registers it in service information, checks accordance with service publicity policy and requests the channel setting function part 34 to set a channel. The channel setting function part 34 monitors a data communication state on the channel to cancel the setting of an unnecessary channel.



LEGAL STATUS
[Date of request for examination] 27.01.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－85059
（Ｐ２００３－８５０５９Ａ）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
G06F 13/00	351	G06F 13/00	351	Z	5B085
15/00	330	15/00	330	A	5B089
H04L 12/46		H04L 12/46		E	5K030
12/66		12/66		B	5K033

審査請求　未請求　請求項の数32　ＯＬ　（全49頁）

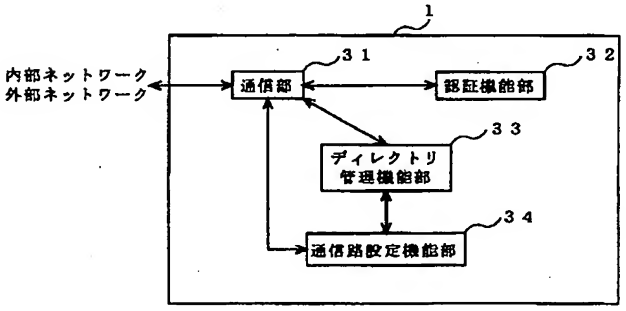
(21)出願番号　特願2002－68762(Ｐ2002－68762)
(22)出願日　平成14年３月13日(2002.3.13)
(31)優先権主張番号　特願2001－76507(P2001－76507)
(32)優先日　平成13年３月16日(2001.3.16)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－199977(P2001－199977)
(32)優先日　平成13年６月29日(2001.6.29)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　古門　健
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　岡田　恭典
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100098291
弁理士　小笠原　史朗

最終頁に続く

(54)【発明の名称】ファイアウォール設定方法およびその装置

(57)【要約】
【課題】　内部ネットワークの端末毎に外部ネットワークからアクセス可能な使用者を限定し、また、上記使用者が選択的に内部ネットワークの端末に接続可能なファイアウォール設定方法およびその装置を提供する。
【解決手段】　ＨＧＷ１は、通信部３１、認証機能部３２、ディレクトリ管理機能部３３および通信路設定機能部３４が設けられている。通信部３１は、ＨＧＷ１へのデータ通信を受信する。また、認証機能部３２は、正当なユーザからのデータか否かを認証する。そして、ディレクトリ管理機能部３３は、サービス登録を受け、サービス情報に登録し、サービス公開ポリシーとの対応をチェックし、通信路設定機能部３４に通信路の設定を依頼する。また、通信路設定機能部３４は、上記通信路のデータ通信状況を監視し、不要な通信路の設定を解除する。



1

【特許請求の範囲】

【請求項１】　外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、

前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、

前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、

前記データ処理部は、

少なくとも前記通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、

前記ユーザ識別データを認証する認証機能部と、

前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証機能部で認証を受けた使用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理機能部と、

前記ディレクトリ管理機能部で前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定機能部とを含む、ファイアウォール装置。

【請求項２】　前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記サーバから送信され少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータによって登録されることを特徴とする、請求項１に記載のファイアウォール装置。

【請求項３】　前記サービスデータは、前記サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、

前記ディレクトリ管理機能部の前記サービス情報は、前記サービス抹消データによって該当するサービスが抹消されることを特徴とする、請求項２に記載のファイアウォール装置。

【請求項４】　前記サービスデータは、前記公開先データを変更する公開先変更データをさらに含み、

前記ディレクトリ管理機能部の前記サービス情報は、前記公開先変更データによって該当するサービスに接続可能な外部の使用者が変更されることを特徴とする、請求項２に記載のファイアウォール装置。

【請求項５】　前記サービスデータは、前記サーバを固定的に識別するサーバ識別情報をさらに含み、

前記ディレクトリ管理機能部は、前記サービス情報を前記サーバ識別情報基づいて関連付けられた前記内部アドレスを更新することを特徴とする、請求項２に記載のファイアウォール装置。

2

【請求項６】　前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記ディレクトリ管理機能部が前記サーバから取得する、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする、請求項１に記載のファイアウォール装置。

【請求項７】　前記ディレクトリ管理機能部は、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて前記サービス情報を登録し、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記サービスデータに係る公開先データを自動生成することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項８】　前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。

【請求項９】　前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。

【請求項１０】　前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データの数が所定数以上である場合

には、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに作成し、一方、当該選出された公開先データの数が所定数以上でない場合には、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。

【請求項１１】　前記ディレクトリ管理機能部への前記サービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１２】　前記通信路設定機能部は、
さらに設定した前記通信路を通るデータを監視し、
予め設定された期間に前記通信路をデータが通らないとき、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１３】　前記通信路設定機能部は、前記外部端末から送信され前記サーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１４】　前記通信路設定機能部は、前記サーバから送信され前記外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１５】　外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、
前記サーバから送信され少なくとも前記サーバが有する内部アドレスとサービス種別とが含まれたサービスデータを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、
前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、
前記データ処理部は、
少なくとも前記サービスデータを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、
前記内部アドレスと前記サービス種別と前記サーバに接続可能な前記外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理機能部と、
前記サービス情報が登録された時に、前記公開先データに該当する前記外部端末が有する外部アドレスと前記サーバの前記内部アドレスとを用いて前記通信路を設定する通信路設定機能部とを含む、ファイアウォール装置。

【請求項１６】　前記ディレクトリ管理機能部に設定される前記公開先データは、前記サーバに対して全ての前記外部端末が接続可能であることを特徴とする、請求項１５に記載のファイアウォール装置。

【請求項１７】　外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、
前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、
前記データ処理ステップで設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続する接続ステップとを備え、
前記データ処理ステップは、
少なくとも前記通信データを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、
前記ユーザ識別データを認証する認証ステップと、
前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証ステップで認証を受けた使用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理ステップと、
前記ディレクトリ管理ステップで前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定ステップとを含む、ファイアウォール設定方法。

【請求項１８】　前記ディレクトリ管理ステップに登録されている前記サービス情報は、前記サーバから送信され少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータによって登録されることを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項１９】　前記サービスデータは、前記サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、
前記ディレクトリ管理ステップの前記サービス情報は、前記サービス抹消データによって該当するサービスが抹消されることを特徴とする、請求項１８に記載のファイアウォール設定方法。

【請求項２０】　前記サービスデータは、前記公開先データを変更する公開先変更データをさらに含み、
前記ディレクトリ管理ステップの前記サービス情報は、前記公開先変更データによって該当するサービスに接続可能な外部の使用者が変更されることを特徴とする、請求項１８に記載のファイアウォール設定方法。

【請求項２１】　前記サービスデータは、前記サーバを

固定的に識別するサーバ識別情報をさらに含み、
前記ディレクトリ管理ステップは、前記サービス情報を前記サーバ識別情報基づいて関連付けられた前記内部アドレスを更新することを特徴とする、請求項１８に記載のファイアウォール設定方法。

【請求項２２】　前記ディレクトリ管理ステップにおいて登録される前記サービス情報は、前記ディレクトリ管理ステップにおいて前記サーバから取得する、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項２３】　前記ディレクトリ管理ステップは、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて前記サービス情報を登録し、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理機ステップは、前記サービスデータに係る公開先データを自動生成することを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項２４】　前記ディレクトリ管理ステップは、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項２３に記載のファイアウォール設定方法。

【請求項２５】　前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに生成することを特徴とする、請求項２３に記載のファイアウォール設定方法。

【請求項２６】　前記ディレクトリ管理ステップは、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データの数が所定数以上である場合には、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに作成し、一方、当該選出された公開先データの数が所定数以上でない場合には、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項２３に記載のファイアウォール設定方法。

【請求項２７】　前記ディレクトリ管理ステップへの前記サービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項２８】　前記通信路設定ステップは、
さらに設定した前記通信路を通るデータを監視し、
予め設定された期間に前記通信路をデータが通らないとき、前記通信路を解除することを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項２９】　前記通信路設定ステップは、前記外部端末から送信され前記サーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項３０】　前記通信路設定ステップは、前記サーバから送信され前記外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１７に記載のファイアウォール設定方法。

【請求項３１】　外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、
前記サーバから送信され少なくとも前記サーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、
前記データ処理ステップで設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続する接続ステップとを備え、
前記データ処理ステップは、
少なくとも前記サービスデータを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、
前記内部アドレスと前記サービス種別と前記サーバに接続可能な前記外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレク

トリ管理ステップと、
前記サービス情報が登録された時に、前記公開先データに該当する前記外部端末が有する外部アドレスと前記サーバの前記内部アドレスとを用いて前記通信路を設定する通信路設定ステップとを含む、ファイアウォール設定方法。

【請求項３２】　前記ディレクトリ管理ステップに設定される前記公開先データは、前記サーバに対して全ての前記外部端末が接続可能であることを特徴とする、請求項３１に記載のファイアウォール設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、外部ネットワークから内部ネットワークへの不正アクセスの遮断に関し、より特定的には、ファイアウォール設定方法およびその装置に関する。

【０００２】

【従来の技術】従来、インターネット等の外部ネットワークとＬＡＮ（Ｌｏｃａｌ　ＡｒｅａＮｅｔｗｏｒｋ）等の内部ネットワークとの間にファイアウォール装置を設置することで、データ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを防御している。このファイアウォール装置の一つにパケットフィルタリングルーター型がある。このパケットフィルタリングルーター型は、内部ネットワークと外部ネットワークとの間で通信されるパケットをある規則に従って転送したりブロックしたりする。しかしながら、このファイアウォール装置も万全ではなく、ネットワークやコンピュータシステムに対する物理的または論理的な侵入や破壊から防止するためのセキュリティ対策の重要性が増している。

【０００３】一方、ローカルアドレス（Ｌｏｃａｌ　Ａｄｄｒｅｓｓ：以下、ＬＡとする）と呼ばれる内部ネットワークのＩＰアドレス（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　Ａｄｄｒｅｓｓ）は、外部ネットワークに対しては有効ではないため、アドレス変換によって外部ネットワークに対して有効なグローバルアドレス（Ｇｌｏｂａｌ　Ａｄｄｒｅｓｓ：以下、ＧＡとする）に変換される。このアドレス変換に改良を加えた技術としてＩＰマスカレード（Ｍａｓｑｕｅｒａｄｅ）がある。このＩＰマスカレードでは、上位プロトコルであるＴＣＰ／ＵＤＰの通信ポート番号を識別し、ＬＡとＧＡとの対応関係を管理することで、１つのＧＡで複数のＬＡが同時に通信可能になる。

【０００４】上記のように内部ネットワークに複数の端末を持ち、ＧＡが共有可能なネットワークアドレス変換方法が、特開２０００－５９４３０号公報に開示されている。この方法は、内部ネットワークの端末と外部ネットワークに接続された端末とがポート番号を変換せずに通信可能とすることを目的としている。この方法による

と、アドレス変換装置にアドレス変換のルールを示す内部テーブルを持たせ、その内部テーブルに、内部ネットワークの端末が通信に用いるポート番号（ＬＰ）および外部ネットワークの端末のＩＰアドレス（ＩＡ）の対（ＬＰ、ＩＡ）と、内部ネットワークの端末のＩＰアドレス（ＬＡ）との対応関係を記憶する。したがってこのアドレス変換装置では、上記内部テーブルの設定によって、内部ネットワークの端末毎に、アクセス可能な外部ネットワークの端末を限定することができる。このようなアドレス変換方法をファイアウォール装置に導入することにより、内部ネットワークの端末毎にアクセス可能な外部ネットワークの端末を限定するというセキュリティ対策が実現できる。

【０００５】一方、さまざまな機器がネットワークで接続される状況において、ユーザがネットワークに接続されている機器を操作して、他のネットワークに接続されている機器の制御情報や状態情報などのサービス情報を入手してその機器を制御することが考えられる。しかし、ネットワークに属しているすべてのユーザに対し、ネットワーク上に提供されているすべてのサービス情報を提供して機器の制御を可能とすることは、ネットワークの安全上好ましくないと考えられる。

【０００６】この問題に対して、従来、ネットワークに属するユーザ毎に異なるサービスの情報を提供するネットワークサービス管理方式が、特開平１１－２７５０７４号公報において開示されている。このネットワークサービス管理方式によれば、ネットワークに発生した情報を、ユーザに対して提供する際、ユーザの業務内容によって、異なる内容を提供する方法を示している。この方式の例では、ユーザはネットワーク管理者、サービス管理者、ユーザに分類され、図５１に示されるネットワークが存在する場合、ネットワーク管理者に対しては、図５２に示されるネットワーク全体の情報を提供し、サービス管理者に対しては、図５３に示されるサービスの情報を提供し、ユーザに対しては、図５４に示されるサーバからユーザへのパスのみを提供する。

【０００７】

【発明が解決しようとする課題】しかしながら、上記アドレス変換方法は、内部ネットワークの端末にアクセス可能な外部ネットワークの端末装置を限定するのみである。つまり、アクセスが許可されている外部ネットワークの端末装置からは正規の使用者に限らず誰でも（悪意のある第三者も）内部ネットワークの端末にアクセス可能である。よって上記アドレス変換方法はセキュリティで劣る面がある。また、複数の使用者が同じ外部ネットワーク端末装置を用いる場合、使用者が変わってもアクセスできる内部ネットワーク端末は同じであり、使用者毎に異なる内部ネットワーク端末に接続することができない。さらに、内部ネットワークに同じサービスを提供するサーバ（例えば、ＦＴＰサーバ）が複数ある場合、

使用者が接続することのできるサーバが１つに固定されてしまい、使用者はこれらのサーバに選択的に接続することができない。また、例えば外部ネットワークの端末装置が電話回線網に接続されている場合などでは外部ネットワークの端末装置を区別するために用いられているＩＡが固定値でないので、上記ＩＡが変更される毎に上記内部テーブルを再設定する必要がある。しかしこの再設定作業は非常に困難であり、固定値でないＩＡに対するアドレス変換は容易ではなかった。

【０００８】それ故に、本発明の目的は、内部ネットワークの端末毎に外部ネットワークからアクセス可能な使用者を限定し、また、上記使用者が選択的に内部ネットワークの端末に接続することを可能にするためのファイアウォール設定方法およびその装置を提供することである。

【０００９】また、上記機器制御方式においては、ネットワークにユーザもしくはサービスなど、新たな構成要素が追加された場合、この構成要素に対して、提供してよい項目を設定しなくてはならない。このことは、家庭内のネットワークについても当てはまり、例えば、ネットワークに対して十分な知識を持たないユーザが、ネットワークに機器を接続する際にその設定を行う必要に迫られる。また、ネットワークに対して提供してよい項目を不用意に選択すると、宅外から無制限にアクセスが可能になるなど、ネットワークの安全上、好ましくない事態が起こりうる。

【００１０】それ故に、本発明の他の目的は、ネットワークに新たな構成要素を加える場合に、単に機器を接続するだけで、好ましいアクセス制限の設定がなされ、セキュリティを確保できる装置および方法を提供することである。

【００１１】

【課題を解決するための手段および発明の効果】上記目的を達成するために、本発明は、以下に述べるような特徴を有している。第１の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、外部端末から送信され少なくとも外部端末が有する外部アドレスと外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理部と、データ処理部で設定された通信路に基づいて、サーバと外部端末とを接続するスイッチ部とを備え、データ処理部は、少なくとも通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、ユーザ識別データを認証する認証機能部と、サーバが有する内部アドレスとサービス種別とサーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、認証機能部で認証を受けた使用者に対して接続可能なサービス情報から選択させるディレクトリ管理機能部と、ディレクトリ管理機能部でサービス情報から選択されたサーバの内部アドレスと外部端末の外部アドレスとを用いて通信路を設定する通信路設定機能部とを含む。

【００１２】第１の発明によれば、外部から接続可能な外部ユーザを限定しユーザ認証を確認した後、その外部ユーザが使用している外部端末の外部アドレスを取得し、その外部アドレスを基にして通信路を設定している。したがって、内部ネットワークのサービスに対して、外部からアクセス可能な外部ユーザを限定して公開することができる。また、上記外部ユーザが使用する外部端末を変更する、あるいは外部ユーザが使用している外部端末の外部アドレスが変わっても同様のアクセスが可能である。また、上記外部ユーザは、通信路を設定する要求をするとき、アクセス可能なサービスを選択的に接続することができ、さらに、同じサービスを内部ネットワーク内で複数のサーバが有していても、上記外部ユーザは上記サーバを選択的に接続することができる。一方、内部ネットワークのサーバに接続可能な外部ユーザを、そのサーバのサービス毎に設定できるため、内部ネットワークの中で同一のサービスを有する複数のサーバに対して、それぞれの異なった接続可能な外部ユーザを設定することにより、サーバ毎のセキュリティレベルを容易に設定することができる。

【００１３】第２の発明は、第１の発明に従属する発明であって、ディレクトリ管理機能部に登録されているサービス情報は、サーバから送信され少なくとも内部アドレスとサービス種別とが含まれたサービスデータによって登録されることを特徴とする。

【００１４】第２の発明によれば、内部ネットワークに接続されているサーバからの指示により、外部ネットワークに公開するサービスを登録および変更することができる。

【００１５】第３の発明は、第２の発明に従属する発明であって、サービスデータは、サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、ディレクトリ管理機能部のサービス情報は、サービス抹消データによって該当するサービスが抹消されることを特徴とする。

【００１６】第３の発明によれば、内部ネットワークのサーバから、そのサーバのサービス毎に外部に提供するか否かを指示することができる。

【００１７】第４の発明は、第２の発明に従属する発明であって、サービスデータは、公開先データを変更する公開先変更データをさらに含み、ディレクトリ管理機能部のサービス情報は、公開先変更データによって該当するサービスに接続可能な外部の使用者が変更されることを特徴とする。

【００１８】第４の発明によれば、内部ネットワークか

ら、そのサーバのサービスに接続可能な外部ユーザを変更し設定することができる。

【００１９】第５の発明は、第２の発明に従属する発明であって、サービスデータは、サーバを固定的に識別するサーバ識別情報をさらに含み、ディレクトリ管理機能部は、サービス情報をサーバ識別情報基づいて関連付けられた内部アドレスを更新することを特徴とする。

【００２０】第５の発明によれば、内部ネットワークのサーバの内部アドレスが変更された場合、上記サーバを識別する固定値を認識することにより、上記サーバと変更された上記内部アドレスとを対応させることができるため、内部アドレス変換時に必要なテーブルの変更を自動的に容易に処理することができる。

【００２１】第６の発明は、第１の発明に従属する発明であって、ディレクトリ管理機能部に登録されているサービス情報は、ディレクトリ管理機能部がサーバから取得する、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする。

【００２２】第６の発明によれば、内部ネットワークに接続されているサーバからの指示によらず、外部ネットワークに公開するサービスを登録および変更することができる。

【００２３】第７の発明は、第１の発明に従属する発明であって、ディレクトリ管理機能部は、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいてサービス情報を登録し、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、サービスデータに係る公開先データを自動生成することを特徴とする。

【００２４】第７の発明によれば、ネットワーク上に新たなサーバが接続されたときなどに、その公開先データが登録されていない場合であっても、これを動的に作成するため、ユーザがその都度設定を行う必要がない。

【００２５】第８の発明は、第７の発明に従属する発明であって、ディレクトリ管理機能部は、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００２６】第８の発明によれば、公開先データが存在しない場合に、予め設定された初期公開先データに基づいて好ましい公開先データを生成することができる。

【００２７】第９の発明は、第７の発明に従属する発明であって、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００２８】第９の発明によれば、公開先データが存在しない場合に、すでに登録されている公開先データに基づいて好ましい公開先データを生成することができる。

【００２９】第１０の発明は、第７の発明に従属する発明であって、ディレクトリ管理機能部は、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データの数が所定数以上である場合には、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに作成し、一方、この選出された公開先データの数が所定数以上でない場合には、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００３０】第１０の発明によれば、公開先データが存在しない場合に、この公開先データを類推するための他の公開先データが、一定数以上存在する場合にはそれらから類推して公開先データを生成し、一方、一定数以上存在しない場合には、初期公開先データに基づいて生成する。よって、公開先データを類推するための材料となる他の公開先データが少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

【００３１】第１１の発明は、第１の発明に従属する発明であって、ディレクトリ管理機能部へのサービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする。

【００３２】第１１の発明によれば、外部ネットワークに提供可能なサービスに対して有効期限を設けており、上記サービスが有効である時のみ一時的に通信路を設定し、しかも上記サービス専用の通信路であるため、さらにセキュリティの向上を実現できる。

【００３３】第１２の発明は、第１の発明に従属する発明であって、通信路設定機能部は、さらに設定した通信路を通るデータを監視し、予め設定された期間に通信路をデータが通らないとき、通信路を解除することを特徴とする。

【００３４】第１２の発明によれば、外部ネットワークに提供可能なサービスの通信路が設けられた後、上記サービスに対して予め設定した期間に上記通信路が外部ユーザによって使用されない場合、上記通信路を解除するため、さらにセキュリティの向上を実現できる。

【００３５】第１３の発明は、第１の発明に従属する発明であって、通信路設定機能部は、外部端末から送信されサーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【００３６】第１４の発明は、第１の発明に従属する発明であって、通信路設定機能部は、サーバから送信され外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【００３７】第１３および第１４の発明によれば、外部端末あるいはサーバからサービス通信終了データを受信することにより通信路を解除するため、サービスの公開が不要な期間の外部からのアクセスを防止することができる。

【００３８】第１５の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、サーバから送信され少なくともサーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理部と、データ処理部で設定された通信路に基づいて、サーバと外部端末とを接続するスイッチ部とを備え、データ処理部は、少なくともサービスデータと通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、内部アドレスとサービス種別とサーバに接続可能な外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理機能部と、サービス情報が登録された時に、公開先データに該当する外部端末の外部アドレスとサーバの内部アドレスとを用いて通信路を設定する通信路設定機能部とを含む。

【００３９】第１５の発明によれば、サーバの指示によってディレクトリ管理機能部にサービス情報を登録されたときに、外部端末からの通信データがなくても、設定された公開先に対して通信路を設定することができる。

【００４０】第１６の発明は、第１５の発明に従属する発明であって、ディレクトリ管理機能部に設定される公開先データは、サーバに対して全ての外部端末が接続可能であることを特徴とする。

【００４１】第１６の発明によれば、内部ネットワークのサーバが有するサービスを、外部端末を限定せずに公開することができる。

【００４２】第１７の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、外部端末から送信され少なくとも外部端末が有する外部アドレスと外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、データ処理ステップで設定された通信路に基づいて、サーバと外部端末とを接続する接続ステップとを備え、データ処理ステップは、少なくとも通信データを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、ユーザ識別データを認証する認証ステップと、サーバが有する内部アドレスとサービス種別とサーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、認証ステップで認証を受けた使用者に対して接続可能なサービス情報から選択させるディレクトリ管理ステップと、ディレクトリ管理ステップでサービス情報から選択されたサーバの内部アドレスと外部端末の外部アドレスとを用いて通信路を設定する通信路設定ステップとを含む。

【００４３】第１８の発明は、第１７の発明に従属する発明であって、ディレクトリ管理ステップに登録されているサービス情報は、サーバから送信され少なくとも内部アドレスとサービス種別とが含まれたサービスデータによって登録されることを特徴とする。

【００４４】第１９の発明は、第１８の発明に従属する発明であって、サービスデータは、サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、ディレクトリ管理ステップのサービス情報は、サービス抹消データによって該当するサービスが抹消されることを特徴とする。

【００４５】第２０の発明は、第１８の発明に従属する発明であって、サービスデータは、公開先データを変更する公開先変更データをさらに含み、ディレクトリ管理ステップのサービス情報は、公開先変更データによって該当するサービスに接続可能な外部の使用者が変更されることを特徴とする。

【００４６】第２１の発明は、第１８の発明に従属する発明であって、サービスデータは、サーバを固定的に識別するサーバ識別情報をさらに含み、ディレクトリ管理ステップは、サービス情報をサーバ識別情報基づいて関連付けられた内部アドレスを更新することを特徴とする。

【００４７】第２２の発明は、第１７の発明に従属する発明であって、ディレクトリ管理ステップにおいて登録されるサービス情報は、ディレクトリ管理ステップにおいてサーバから取得する、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする。

15

【００４８】第２３の発明は、第１７の発明に従属する発明であって、ディレクトリ管理ステップは、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいてサービス情報を登録し、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理機ステップは、サービスデータに係る公開先データを自動生成することを特徴とする。

【００４９】第２４の発明は、第２３の発明に従属する発明であって、ディレクトリ管理ステップは、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００５０】第２５の発明は、第２３の発明に従属する発明であって、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００５１】第２６の発明は、第２３の発明に従属する発明であって、ディレクトリ管理ステップは、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データの数が所定数以上である場合には、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに作成し、一方、この選出された公開先データの数が所定数以上でない場合には、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【００５２】第２７の発明は、第１７の発明に従属する発明であって、ディレクトリ管理ステップへのサービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする。

16

【００５３】第２８の発明は、第１７の発明に従属する発明であって、通信路設定ステップは、さらに設定した通信路を通るデータを監視し、予め設定された期間に通信路をデータが通らないとき、通信路を解除することを特徴とする。

【００５４】第２９の発明は、第１７の発明に従属する発明であって、通信路設定ステップは、外部端末から送信されサーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【００５５】第３０の発明は、第１７の発明に従属する発明であって、通信路設定ステップは、サーバから送信され外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【００５６】第３１の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、サーバから送信され少なくともサーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、データ処理ステップで設定された通信路に基づいて、サーバと外部端末とを接続する接続ステップとを備え、データ処理ステップは、少なくともサービスデータを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、内部アドレスとサービス種別とサーバに接続可能な外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理ステップと、サービス情報が登録された時に、公開先データに該当する外部端末が有する外部アドレスとサーバの内部アドレスとを用いて通信路を設定する通信路設定ステップとを含む。

【００５７】第３２の発明は、第３１の発明に従属する発明であって、ディレクトリ管理ステップに設定される公開先データは、サーバに対して全ての外部端末が接続可能であることを特徴とする。

【００５８】

【発明の実施の形態】（第１の実施形態）図１は、本発明の第１の実施形態に係るファイアウォール装置の基本的構成を示す図である。以下、図１を用いて、当該実施形態について説明する。

【００５９】図１において、当該実施形態では、内部ネットワークとして、ホームゲートウエイ装置（以下、ＨＧＷとする）１に複数のサーバ２－１～ｎがバス接続されてＬＡＮが構築されている。一方、ＨＧＷ１は、外部ネットワークとして、インターネット網を介して複数の外部端末３を接続されている。なお、内部ネットワークには、サーバ２－１～ｎの他に、内部端末が接続されていてもかまわないし、外部ネットワークには、外部端末

３の他に、外部サーバが接続されていてもかまわない。

【００６０】ここで、ＨＧＷ１は、外部ネットワークとの送受信に用いられるグローバルＩＰアドレス（ＧＡ）が付与されており、複数のポート番号（ＧＰ）を用いてパケットの送受信を行う。また、サーバ２－１～ｎは、それぞれに固有のローカルＩＰアドレス（ＬＡ）１～ｎとサーバ２－１～ｎが提供するサービスに応じて、クライアントとなる端末からの通信を受信するポート番号（ＬＰ）１～ｎが設定されている。さらに、外部端末３は、外部ネットワークとの送受信に用いられるグローバルＩＰアドレス（ＩＡ）と送受信に使用するポート番号（ＩＰ）とが付与されている。

【００６１】次に、前述したＨＧＷ１の内部ハードウエアの基本構成について説明する。なお、図２は、当該実施形態に係るＨＧＷ１の内部ハードウエア基本構成を示すブロック図である。以下、図２を参照して、ＨＧＷ１について説明する。

【００６２】図２において、ＨＧＷ１は、ＣＰＵ１０とメモリ１１とＩＰスイッチ部２０とを備えている。また、ＩＰスイッチ部２０は、コントローラ２１、メモリ、２２、ＩＰフィルタ機能部２３、フォワーディング機能部２４、アドレス変換機能部２５およびＰＨＹ・ＭＡＣ（Ｐｈｙｓｉｃａｌ　Ｌａｙｅｒ　Ｐｒｏｔｏｃｏｌ・Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）機能部２６ａおよび２６ｂを含んでいる。ＣＰＵ１０は、各機能部の制御や送受信するデータの処理等を行い、メモリ１１には、ＨＧＷ１の動作プログラムやデータ等が格納されている。また、コントローラ２１は、ＣＰＵ１０から設定情報を受け取り、上記設定情報に基づいてＩＰフィルタ機能部２３、フォワーディング機能部２４およびアドレス変換機能部２５の設定を行う。また、コントローラ２１は、外部ネットワークおよび内部ネットワークに対してデータの送受信を行うＰＨＹ・ＭＡＣ機能部２６で受信したデータに対して、ＩＰフィルタ機能部２３、フォワーディング機能部２４およびアドレス変換機能部２５に処理を指示する。メモリ２２は、ＰＨＹ・ＭＡＣ機能部２６で受信したパケットデータを一時的に格納する。ＩＰフィルタ機能部２３は、その内部にフィルタ条件格納用のレジスタを有し、上記レジスタに格納されたフィルタ条件に基づいて、メモリ２２に格納された上記パケットデータのチェックを行う。なお、上記パケットデータが、上記フィルタ条件に対して許可されないデータである場合、ＩＰフィルタ機能部２３は、上記パケットデータを廃棄する。フォワーディング機能部２４は、その内部にフォワーディング情報格納用のレジスタを有し、上記レジスタに格納された上記情報に基づいて、メモリ２２に格納されたパケットデータの転送先ＰＨＹ・ＭＡＣ機能部２６を決定し、上記パケットデータの転送を制御する。アドレス変換機能部２５は、その内部にアドレス変換情報格納用のレジスタを有し、上記レジスタに格納された上記アドレス変換情報に基づいて、メモリ２２に格納されたパケットデータに対してＩＰアドレスの変換を行う。

【００６３】次に、前述したＨＧＷ１のソフトウエアの基本構成について説明する。なお、図３は、当該実施形態に係るＨＧＷ１のソフトウエア基本構成を示すブロック図である。以下、図３を参照して、ＨＧＷ１について説明する。

【００６４】図３において、ＨＧＷ１は、通信部３１、認証機能部３２、ディレクトリ管理機能部３３および通信路設定機能部３４が設けられている。通信部３１は、外部端末３またはサーバ２からＨＧＷ１へのデータ通信を受信し、データ内容によって各機能部に処理を依頼する。また、認証機能部３２は、認証情報を管理し、上記データが正当なユーザからのデータか否かを認証する。そして、ディレクトリ管理機能部３３は、サーバ２からのサービス登録を受け、サービス情報（詳細は、後述する）を登録および管理し、上記サービス情報とサービス公開ポリシー（詳細は、後述する）との対応をチェックし、必要に応じて通信路設定機能部３４に通信路の設定を依頼する。また、通信路設定機能部３４は、ＩＰフィルタ機能部２３、フォワーディング機能部２４、アドレス変換機能部２５およびアプリケーションＧＷ等を設定し、通信路を設定する。また、通信路設定機能部３４は、上記通信路のデータ通信状況を監視し、不要な通信路の設定を解除する。

【００６５】ここで、当該ファイアウォール装置は、ＨＧＷ１のスイッチ部２０に通信路を設定することにより外部ネットワークの外部端末３と内部ネットワークのサーバ２とが接続可能となり、サーバ２のサービスが外部に公開される。上記内部ネットワークのサーバ２から公開可能なサービスについては、サービス情報（詳細は、後述する）として管理されており、上記サービス情報に基づいて、通信路が設定される。当該ファイアウォール装置では、上記公開の方法として、外部ユーザの認証を必要としない「認証なし」のサービスと、外部ユーザの認証を必要とする「認証後公開」のサービスと、外部ネットワークに公開されない「非公開」のサービスとを設定できる。上記「認証なし」のサービスは、上記サービス情報にそのサービスが登録された時点で通信路が設定され、外部ネットワークからどのようなユーザでも接続可能である。また、上記「認証後公開」のサービスは、許可されたユーザがそのサービスへ接続を希望した時点で通信路が一時的に設定され、許可されたユーザのみが接続可能である。さらに、上記公開可能なサービスは、それぞれ有効期限を有しており、その有効期限が終了した場合、上記サービス情報から抹消される。以下、上述したそれぞれの通信路設定処理について説明する。

【００６６】まず、ＨＧＷ１で行われる上記サービス情報の設定処理および上記「認証なし」のサービスに対す

る通信路設定処理について説明する。なお、図４および図５はＨＧＷ１で行われる通信路設定処理の動作を示すフローチャートであり、図８～図１０はＨＧＷ１で行われる通信路設定処理の時に作成・使用される情報テーブルを示している。以下、図４、図５および図８～図１０を参照して、通信路設定処理について説明する。

【００６７】図４において、ＨＧＷ１は、ＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、ＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）およびＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）等のサービスをディレクトリ管理機能部３３に登録するため、サーバ２からサービス登録を受信する（ステップＳ１０１）。

【００６８】なお、ここではサーバ２がＨＧＷ１に対してサービス登録を行う場合について説明しているが、これに限らず、ＨＧＷ１がサーバ２よりサービス情報を取得するようにしても構わない。その場合、ディレクトリ管理機能部３３は、図４のステップＳ１０１の代わりに、図１３に示す処理を実行する。つまり、ディレクトリ管理機能部３３は、まず内部ネットワークに接続されているサーバ２に対してポートスキャンを行い、サーバ２が使用しているポートを検索する（Ｓ２０１）。この結果、サーバが使用しているポートが予めサービスの仕様によって決定されているポート（ウェルノウンポート：ｗｅｌｌ－ｋｎｏｗｎ　ｐｏｒｔ）であった場合には、そのポートに対応するサービスをサーバが提供していることが分かる（Ｓ２０２）。なおサーバが使用しているポートがウェルノウンポートでない場合には、ポートスキャンに対する応答メッセージを確認することにより、サーバが提供しているサービスを検知することができる。このとき、ＨＧＷ１が新規サーバの接続を知る方法としては、ＤＨＣＰによる新規ＩＰアドレスの割当て時に検出する方法や、ＡＲＰパケットのＭＡＣアドレスを監視することによって検出する方法等がある。加えて、ＩＰｏｖｅｒ１３９４を使用する場合のように、新規の機器接続を検出可能なネットワークを使用する場合には、ＨＧＷ１は、ネットワークの仕組みを用いて新規サーバの接続を検出し、このサーバからサービス情報を取得する。

【００６９】次に、ＨＧＷ１は、受信した上記サービス登録のサービスに対して、ディレクトリ管理機能部３３に格納されているサービス情報を参照して、上記サービスのサービス種別とサーバ識別情報との対が、既に上記サービス情報に登録済みか否か判断する（ステップＳ１０２）。

【００７０】図８は、ディレクトリ管理機能部３３に格納されているサービス情報の一例を示す図である。サービス情報は、内部ネットワークのサーバ２がどのようなサービスを外部に公開可能であるかを示す情報であり、スイッチ部２０の通信路を設定するための情報も管理されている。上記サービス情報は、サービス名、サービスアドレス、プロトコル、外部公開ポート番号（ＧＰ）、現在の公開先、サービス有効期間および状態を、互いに関連付けたテーブルとしてディレクトリ管理機能部３３に格納されている。サービス名は、外部に公開するサービス種別を示しており、サービスアドレスは、サーバ２のサーバ識別情報、ＬＡおよびＬＰを示している。ここで、サーバ識別情報とは、ＭＡＣアドレスやサーバ装置のシリアル番号等のサーバ２を識別する固定値である。また、現在の公開先は、ＨＧＷ１のスイッチ部２０で通信路が設定されている公開先を示している。なお、外部から接続可能なユーザまたは端末を限定して公開されている場合、現在の公開先は、そのユーザ名と外部端末３のＩＡおよびＩＰとが示される。サービス有効期間は、それぞれに予め設定されたサービス種別毎の公開有効期間の残存時間を示している。また、状態は、サービスが現在使用可であるか否かを示している。なお、このサービス情報へのサービス登録は、同じサービス種別であってもサーバ識別情報が異なる場合、登録済みとは判断されないため、新しいサービスとして処理される。したがって、上記サービス情報には、サーバ２毎に有効なサービスが登録されることになる。

【００７１】ステップＳ１０２で、上記サービス登録のサービスに対してサービス種別とサーバ識別情報との対が、上記サービス情報に登録されていない場合、ＨＧＷ１は、予めディレクトリ管理機能部３３に設定されているサービス基本公開ポリシーに基づいて、サービス詳細公開ポリシーを設定する（ステップＳ１０９）。

【００７２】図９はディレクトリ管理機能部３３に予め設定されているサービス基本公開ポリシーの一例を示す図であり、図１０はディレクトリ管理機能部３３に設定されるサービス詳細公開ポリシーの一例を示す図である。まず、サービス基本公開ポリシーは、それぞれのサービス種別に対する外部から接続可能な条件として、公開先相手、公開条件および公開ポートが、予めディレクトリ管理機能部３３に設定されている。なお、公開先相手は、外部から接続可能なユーザを限定して公開する場合、そのユーザ名が設定される。また、接続可能な外部端末３を限定して公開する場合、その端末のＩＡが設定される。そして、公開条件が「認証なし」で公開先相手が「全て公開」の場合、そのサービスは外部のどのようなユーザからも接続が可能となり、上記サービス情報にそのサービスが登録された時点でスイッチ部２０の通信路が設定される。また、公開条件が「認証なし」で公開先相手が外部端末３のＩＡの場合、上記サービス情報にそのサービスが登録された時点でスイッチ部２０の通信路が設定される。一方、公開条件が「認証後公開」の場合、公開先相手に登録されたユーザがそのサービスに接続を希望した時点でスイッチ部２０の通信路が一時的に設定される。ステップＳ１０９では、上記基本公開ポリ

シーに基づいて、サーバ２毎に、それぞれサービス種別に対する上記接続条件をサービス詳細公開ポリシーとして設定する。したがって、上記サービス詳細公開ポリシーは、それぞれのサーバ２に対して上記接続条件が設定され、サーバ２の管理者によって環境に応じた上記接続条件に変更することが可能である。なお、上記接続条件の変更が不要な場合、サービス詳細公開ポリシーには、サービス基本公開ポリシーの上記接続条件が適用される。また、サービス基本公開ポリシーに該当するサービス種別がない場合、公開先相手は「非公開」として設定される。

【００７３】次に、ＨＧＷ１は、上記サービス登録のサービスを上記サービス情報にエントリ追加し、上記サービスの内容を上記サービス情報に設定する（ステップＳ１１０）。そして、ＨＧＷ１は、上記サービス詳細公開ポリシーを参照し、上記サービスの公開条件が「認証なし」か否かを判断する（ステップＳ１１１）。ＨＧＷ１は、上記公開条件が「認証なし」でない場合、フローを終了し、上記公開条件が「認証なし」の場合、さらに上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する（ステップＳ１１２）。そして、ＨＧＷ１は、上記公開ポートが「指定なし」の場合、空ポート番号（ＧＰ）を設定した後（ステップＳ１１３）、ステップＳ１１６に進む。一方、上記公開ポートが指定されている場合、ＨＧＷ１は、指定されているポート（ＧＰ）が使用可か否かを判断する（ステップＳ１１４）。そして、ＨＧＷ１は、指定されているＧＰが使用可の場合、そのＧＰを取得した後（ステップＳ１１５）、ステップＳ１１６に進む。次に、ＨＧＷ１は、上記サービス情報を参照して、上記サービスの状態が「使用可」か否かを判断し（ステップＳ１１６）、上記状態が「使用不可」の場合、フローを終了する。上記状態が「使用可」で公開先相手が「全て公開」の場合、ＨＧＷ１は、上記サービスに対して内部アドレス情報（ＬＡおよびＬＰ）および外部公開用アドレス情報（ＨＧＷ１のＧＡおよび上記ＧＰ）を取得してＩＰフィルタ機能部２３およびアドレス変換機能部２５を設定することによりスイッチ部２０の通信路を設定し（ステップＳ１１７）、フローを終了する。なお、ステップＳ１１７で、上記状態が「使用可」で公開先相手が外部端末３のＩＡの場合、ＨＧＷ１は、上記サービスに対して内部アドレス情報（ＬＡおよびＬＰ）、外部公開用アドレス情報（ＨＧＷ１のＧＡおよび上記ＧＰ）および外部端末３のアドレス情報（外部端末３のＩＡおよびＩＰ）を取得してＩＰフィルタ機能部２３およびアドレス変換機能部２５を設定することによりスイッチ部２０の通信路を設定する。

【００７４】一方、ステップＳ１１４で、指定されているＧＰが使用不可の場合、ＨＧＷ１は、上記サービス情報を参照して該当する上記サービスの状態を「使用不可」に設定し（ステップＳ１１８）、フローを終了する。これは、指定されたポート番号ＧＰを用いて、アドレス変換機能部２５が設定できないことを意味する。例えば、同一の外部端末３が、ＦＴＰサービスに対して同一のポート番号を用いて複数の内部ネットワークのサーバ２に通信を要求した場合、アドレス変換機能部２５では、アドレス変換の条件を設定できないため、指定されているＧＰが使用不可と判断される。

【００７５】一方、ステップＳ１０２で、上記サービスのサービス種別とサーバ識別情報との対が、既に上記サービス情報に登録済みの場合、ＨＧＷ１は、上記サービス情報を参照し、該当する上記サービスのサービス有効期間を再設定する（ステップＳ１０３）。このサービス有効期間を再設定は、予め設定されたサービス種別毎の公開有効期間に初期化されてもいいし、新たに上記公開有効期間を設定してもかまわない。次に、ＨＧＷ１は、上記サービスの状態が変更されている場合、状態変更処理を行う（ステップＳ１０４）。このステップＳ１０４の詳細については、後述する。次に、ＨＧＷ１は、上記サービス情報を参照し、上記サービスに対するＬＡあるいはＬＰが変更されているか否かを判断し（ステップＳ１０５）、変更されていない場合、フローを終了する。ステップＳ１０５で、上記サービスのＬＡあるいはＬＰが変更されていると判断された場合、ＨＧＷ１は、上記サービスに対して、上記サービス情報に示されているサービスアドレスのＬＡあるいはＬＰを更新する（ステップＳ１０６）。その後、ＨＧＷ１は、上記サービスに対する上記サービス情報の現在の公開先が指定されているか否かを判断し（ステップＳ１０７）、指定されている場合、スイッチ部２０に設定されている通信路を抹消し（ステップＳ１０８）、前述のステップＳ１１６に進む。一方、ステップＳ１０７で、現在の公開先が指定されていない場合、ＨＧＷ１は、フローを終了する。

【００７６】次に、前述したステップＳ１０４についての詳細動作を説明する。なお、図５は、ステップＳ１０４のサブルーチンを示している。図５において、ＨＧＷ１は、上記サービス情報を参照し、上記サービス登録によって状態が変化するか否かを判断する（ステップＳ２０１）。ＨＧＷ１は、上記サービス登録によって状態が変化しない場合、フローを終了する。一方、上記状態が上記サービス登録によって使用可→使用不可あるいは使用不可→使用可に変化する場合、ＨＧＷ１は、上記状態が使用不可→使用可に変化するか否かを判断する（ステップＳ２０２）。上記サービス登録によって状態が使用不可→使用可に変化する場合、ＨＧＷ１は、上記サービス情報の上記サービスの状態を「使用可」に更新する（ステップＳ２０３）。そして、ＨＧＷ１は、上記サービスに対して、上記サービス詳細公開ポリシーの公開条件が「認証なし」か否か（ステップＳ２０４）と、公開先相手が指定されているか否かとを判断する（ステップ

Ｓ２０５）。公開条件が「認証なし」で、公開先相手が指定されている場合、ＨＧＷ１は、上記指定されている公開先相手を上記サービス情報の現在の公開先に設定する（ステップＳ２０６）。その後、ＨＧＷ１は、上記サービスに対して、上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する（ステップＳ２０７）。そして、ＨＧＷ１は、上記公開ポートが「指定なし」の場合、空ポート番号（ＧＰ）を取得した後（ステップＳ２０８）ステップＳ２１１に進み、上記公開ポートが指定されている場合、指定されているポート（ＧＰ）が使用可か否かを判断する（ステップＳ２０９）。そして、ＨＧＷ１は、指定されているＧＰが使用可の場合、そのＧＰを取得する（ステップＳ２１０）。その後、ＨＧＷ１は、公開先相手に外部端末３のＩＡが指定されている場合、上記サービスに対して、公開先のアドレス情報（外部端末３のＩＡおよびＩＰ）と内部アドレス情報（ＬＡおよびＬＰ）と、外部公開用アドレス情報（ＨＧＷ１のＧＡおよび上記ＧＰ）とを取得してＩＰフィルタ機能部２３およびアドレス変換機能部２５を設定することによりスイッチ部２０の通信路を設定し（ステップＳ２１１）、フローを終了する。なお、ＨＧＷ１は、公開先相手に「全て公開」が指定されている場合、上記サービスに対して、内部アドレス情報（ＬＡおよびＬＰ）と、外部公開用アドレス情報（ＨＧＷ１のＧＡおよび上記ＧＰ）とを取得してＩＰフィルタ機能部２３およびアドレス変換機能部２５を設定することによりスイッチ部２０の通信路を設定する。このようにして、サービスの状態が、「使用不可」→「使用可」に変更された場合、スイッチ部２０の通信路が設定される。一方、ステップＳ２０９で、指定されているＧＰが使用不可の場合、ＨＧＷ１は、上記サービス情報を参照して、上記サービスの状態を「使用不可」に設定し（ステップＳ２１２）、フローを終了する。

【００７７】一方、ステップＳ２０２で上記サービス登録によって状態が使用可→使用不可に変化する場合、ＨＧＷ１は、上記サービス情報を参照して、該当するサービスの状態を「使用不可」に設定する（ステップＳ２１３）。その後、ＨＧＷ１は、上記サービスに対して、スイッチ部２０で設定されていた通信路（ステップＳ２１４）および上記サービス情報の現在の公開先を抹消し（ステップＳ２１５）、フローを終了する。したがって、サービスの状態が、「使用可」→「使用不可」に変更された場合、スイッチ部２０の通信路が遮断される。

【００７８】次に、上記サービス詳細公開ポリシーの公開条件が「認証後公開」となっているサービス（以下、認証サービスとする）に対して、スイッチ部２０の通信路が外部から設定される動作について説明する。なお、図６は、ＨＧＷ１が、認証サービスに対して、上記通信路が外部から設定される動作を示すフローチャートである。

【００７９】図６において、ＨＧＷ１は、外部端末３からＨＧＷ１の専用ＧＰ（典型的には、ポート８０）を介して、通信路設定要求を受信する（ステップＳ３０１）。次に、ＨＧＷ１は、上記通信路設定要求を送信した外部端末３に対して、ユーザ認証を要求する（ステップＳ３０２）。これは、典型的には、ユーザ名とパスワードの入力を要求することによってユーザ認証を要求する。そして、ＨＧＷ１は、上記ユーザ認証要求に対する入力結果を上記外部端末３から受信し、認証登録部３２で上記入力結果が予め認証登録部３２に記憶されているユーザ登録と一致するか否かを判断する（ステップＳ３０３）。上記入力結果が上記ユーザ登録と一致しない場合、ＨＧＷ１はフローを終了する。一方、上記入力結果が上記ユーザ登録と一致する場合、ＨＧＷ１は、上記ユーザに対して、前述したサービス詳細公開ポリシーに公開先相手として許可されており、かつ前述したサービス情報の状態が使用可である認証サービスの一覧を上記外部端末３に送信する（ステップＳ３０４）。次に、ＨＧＷ１は、上記一覧からユーザによって選択された認証サービスおよびその認証サービスを提供するサーバの選択結果を受信する（ステップＳ３０５）。

【００８０】その後、ＨＧＷ１は、上記認証サービスに対して、上記サービス情報の状態は使用可か否か（ステップＳ３０６）、ステップＳ３０３と同様のユーザ認証の再確認（ステップＳ３０７）、および上記ユーザが上記サービス詳細公開ポリシーの公開先相手として許可されているか否か（ステップＳ３０８）を再確認する。これは、上記一覧から選択されなかった場合等を想定したセキュリティ対策である。なお、ステップＳ３０７のユーザパスワード確認は、ステップＳ３０３とは異なった上記認証サービス固有のパスワードを確認に使用してもかまわない。なお、ＨＧＷ１は、ステップＳ３０６～Ｓ３０８で不可と判定した場合、全てフローを終了する。

【００８１】ステップＳ３０８で、上記ユーザが公開先相手として許可されている場合、ＨＧＷ１は、上記認証サービスに対して、上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する（ステップＳ３０９）。そして、ＨＧＷ１は、上記公開ポートが「指定なし」の場合、空ポート番号（ＧＰ）を取得した後（ステップＳ３１０）ステップＳ３１３に進む。一方、上記公開ポートが指定されている場合、ＨＧＷ１は、指定されているポート（ＧＰ）が使用可か否かを判断する（ステップＳ３１１）。そして、ＨＧＷ１は、指定されているＧＰが使用可の場合、そのＧＰを取得した後（ステップＳ３１２）、上記認証サービスに対する内部アドレス情報（ＬＡおよびＬＰ）、外部公開用アドレス情報（ＨＧＷ１のＧＡおよび上記ＧＰ）および外部端末３のアドレス情報（外部端末３のＩＡおよびＩＰ）を取得してＩＰフィルタ機能部２３およびアドレス変換機能部２５を設定することによりスイッチ部２０の通信路を一時

的に設定する（ステップＳ３１３）。そして、ＨＧＷ１は、上記サービス情報の現在の公開先に上記ユーザ名と公開先のアドレス情報（外部端末３のＩＡおよびＩＰ）とを追加する（Ｓ３１４）。なお、上記外部端末３のアドレス情報は、上記通信路設定要求データの送信元ＩＰアドレスを取得してもいいし、上記ユーザによって新たに指定されてもかまわない。

【００８２】このように、「認証後公開」のサービスは、許可されたユーザのみ接続が可能であり、ユーザ認証後は、上記ユーザが現在使用している外部端末３のアドレス情報に基づいて、スイッチ部２０の通信路が設定される。その後、ＨＧＷ１は、外部端末３に対して、通信路を設定したサーバ２との通信に使用するポート番号を通知し（ステップＳ３１５）、フローを終了する。一方、ステップＳ３１１で、指定されているＧＰが使用不可の場合、上記サービス情報を参照して、上記認証サービスの状態を「使用不可」に設定し（ステップＳ３１６）、外部端末３に上記サービスが使用不可であることを通知した後、フローを終了する。

【００８３】ここで、上述のように上記ユーザに対して設定された通信路は、上記サービスに対して一時的に通信路を設定される。ＨＧＷ１の通信路設定機能部３４は、上記通信路のデータ通信量を監視し予め設定された期間内にデータ通信がない場合、上記通信路を抹消する。なお、上記データ通信量の監視は、スイッチ部２０で行い、その結果を通信路設定機能部３４に通知してもかまわない。さらに、ＨＧＷ１は、上記サービスの接続が終了したことを上記ユーザが使用する外部端末３あるいはサーバ２から通知させ、その通知を受信することによっても上記通信路を抹消する。

【００８４】次に、ＨＧＷ１で行われるサービス有効期限管理について説明する。なお、図７は、ＨＧＷ１が行うサービス有効期限管理の動作を示すフローチャートである。以下、図７を参照して、サービス有効期限管理について説明する。

【００８５】図７において、ＨＧＷ１は、上記サービス情報に登録されているそれぞれのサービスに対してサービス有効期間が有効か否かを判断する（ステップＳ４０１）。サービス有効期間が有効である場合、ＨＧＷ１は、フローを終了し、サービス有効期間のチェックを継続する。一方、サービス有効期間が終了しているサービスがある場合、ＨＧＷ１は、そのサービスに対して上記サービス情報の状態を「使用不可」に設定する（ステップＳ４０２）。そして、ＨＧＷ１は、上記サービスに対して、スイッチ部２０に設けられている通信路（ステップＳ４０３）と、上記サービス情報の現在の公開先とを抹消する（ステップＳ４０４）。次に、ＨＧＷ１は、上記サービスに対して、エントリ削除タイマＴを起動させ（ステップＳ４０５）、予め設定されている削除猶予時間が経過するまで待機する（ステップＳ３０６）。上記

待機中に前述したサービス登録が行われ、上記サービスに対してサービス有効期間の再設定が行われた場合、ＨＧＷ１は、フローを終了する（ステップＳ４０７）。このように、上記削除猶予時間を設けることにより、再度状態が使用可になった場合、外部からは同じポート番号（ＧＰ）で接続することが可能である。一方、上記エントリ削除タイマＴが上記削除猶予時間を経過した場合、ＨＧＷ１は、上記サービスを上記サービス情報のエントリから削除し（ステップＳ４０８）、フローを終了する。したがって、サービス有効期間が無効になった場合、上記サービスは、上記削除猶予時間を経て上記サービス情報から抹消される。

【００８６】次に、前述のように設定された通信路に対して、スイッチ部２０が設定される動作について説明する。まず、当該実施形態では、内部ネットワークから外部ネットワークへの通信は、動的ＩＰマスカレードが自動的に適用され、ディレクトリ管理機能部３３がスイッチ部２０の通信路の設定を行わなくても通信が可能となるように、ＩＰフィルタ機能部２３およびアドレス変換機能部２５が設定されている。なお、図１１は、内部ネットワークから外部ネットワークへの通信を許可するためのＩＰフィルタ機能部２３に設定されるパケットフィルタの情報を示す図である。

【００８７】図１１において、方向は、ＰＨＹ・ＭＡＣ機能部２６が送信する方向を示し、「外」の場合、内部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ｂで受信し、外部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ａから送信されるパケットであることを示している。また、「内」の場合、外部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ａで受信し、内部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ｂから送信されるパケットであることを示している。そして、ＳＡ（ソースアドレス）とＤＡ（デスティネーションアドレス）とは、それぞれパケットに付与されている送信元アドレスと送信先アドレスとを示している。また、ＳＰ（ソースポート）とＤＰ（デスティネーションポート）とは、それぞれパケットに付与された送信元ポート番号と送信先ポート番号とを示している。また、ＡＣＫ（Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ Ｆｌａｇ）は、ＡＣＫをチェックするか否かを示している。なお、ＡＣＫは、接続を確立するパケットではセットされず、それ以降のパケットでセットされている。このＩＰフィルタ機能部２３に設定されている情報は、デフォルト設定ＡおよびＢとして予め設定されている。したがって、内部ネットワークのサーバ２からＨＧＷ１へ通信を開始するパケットを送信した場合、デフォルト設定Ａによってパケットフィルタの通過が許可される。そして、外部ネットワークの外部端末３からＨＧＷ１への応答は、デフォルト設定Ｂによってパケットフィルタの通過が許可される。一方、外部ネットワークの外部端末

27

３からＨＧＷ１へ通信を開始するパケットを送信した場合、そのパケットにＡＣＫがセットされていないため、デフォルト設定Ｂによって通過を拒否される。すなわち、新たなパケットフィルタの設定を追加しない限り外部ネットワークから内部ネットワークに通信を開始することができない。

【００８８】次に、ＦＴＰサービスを公開する場合、スイッチ部２０のＩＰフィルタ機能部２３およびアドレス変換機能部２５に設定される情報について説明する。なお、図１２（ａ）はＦＴＰサービスの通信シーケンスを示す図であり、図１２（ｂ）はディレクトリ管理機能部３３によってアドレス変換機能部２５に設定されるアドレス変換テーブルを示す図であり、図１２（ｃ）はディレクトリ管理機能部３３によってＩＰフィルタ機能部２３に設定されるパケットフィルタを示す図である。以下、図１２を参照して、ＦＴＰサービスの通信路設定要求が行われた場合、制御用セッションのパケットが伝送する形態について説明する。

【００８９】まず、外部端末３から、ソースアドレスＩＡ、ソースポート番号ＩＰ１、デスティネーションアドレスＧＡおよびデスティネーションポート番号２１が付与されたパケットが送信される。次に、ＨＧＷ１は、上記パケットを受信し、アドレス変換機能部２５のアドレス変換テーブルの条件Ｃを適用することにより、デスティネーションアドレスＧＡおよびデスティネーションポート番号２１をそれぞれＦＴＰサーバ２のＬＡおよびＬＰ２１に変換する。その後、ＩＰフィルタ機能部２３は、上記パケットに対してパケットフィルタの条件Ｅを適用することによってフィルタリング処理を実行し、上記パケットの通過を許可する。次に、フォワーディング機能部２４によって、上記パケットは、内部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ｂを介してＦＴＰサーバ２へ送信される。

【００９０】そして、ＦＴＰサーバ２は、外部端末３からの上記パケットを受信した後、ソースアドレスＬＡ、ソースポート番号２１、デスティネーションアドレスＩＡおよびデスティネーションポート番号ＩＰ１が付与された応答パケットをＨＧＷ１へ送信する。次に、ＨＧＷ１は、上記応答パケットを受信し、上記応答パケットに対してＩＰフィルタ機能部２３のパケットフィルタのデフォルト設定Ａを適用することによってフィルタリング処理を実行し、上記応答パケットの通過を許可する。その後、アドレス変換機能部２５のアドレス変換テーブルの条件Ｄを適用することにより、ソースアドレスＬＡおよびソースポート番号２１をそれぞれＨＧＷ１のＧＡおよびＧＰ２１に変換する。次に、フォワーディング機能部２４によって、上記応答パケットは、外部ネットワークと接続されているＰＨＹ・ＭＡＣ機能部２６ａを介して外部端末３へ送信される。

【００９１】また、上記ＦＴＰサービスでは、上記制御

28

用セッションの他に、データ用セッションが外部端末３とＦＴＰサーバ２との間でポート番号２０を用いて確立される。このデータ用セッションの確立は、ＦＴＰサーバ２から通信を開始することにより行われるため、動的ＩＰマスカレードとデフォルトのフィルタリング設定により、ディレクトリ管理機能部３３によって特別な設定が行われなくても内部ネットワークからの通信が可能となる。

【００９２】なお、前述したＦＴＰサービスによる伝送形態では、内部ネットワークから外部ネットワークへの通信は、動的ＩＰマスカレードが自動的に適用され、ディレクトリ管理機能部３３がスイッチ部２０の設定を行わなくても内部からの通信が可能となるように、ＩＰフィルタ機能部２３およびアドレス変換機能部２５が設定されている。しかしながら、ＨＧＷ１のセキュリティをさらに高めるために、上記動的ＩＰマスカレードやデフォルトのパケットフィルタの設定を行わなくてもかまわない。このような場合、外部ネットワークの外部端末３からＦＴＰサーバ２にアクセスするためには、ＦＴＰサーバ２のＬＰに対応するアドレス変換とパケットフィルタとの一連の設定が必要となる。これは、サービス種別に応じてＬＰに対応する一連の設定用テンプレートを予め用意しておくことで、容易にＩＰフィルタ機能部２３およびアドレス変換機能部２５の設定を行うことができる。なお、上記設定用テンプレートがないサービス種別のサービスが登録された場合、上記設定用テンプレートをサーバ２あるいは外部ネットワークの定められたサーバから取得することによって、ＩＰフィルタ機能部２３およびアドレス変換機能部２５の設定を行うことができる。

【００９３】なお、当該実施形態では、内部ネットワークを１つのネットワークとして説明したが、ＨＧＷ１に対して複数の内部ネットワークを接続してもかまわない。これは、スイッチ部２０に第３のＰＨＹ・ＭＡＣ機能部２６を増設し、上記第３のＰＨＹ・ＭＡＣ機能部２６に外部ネットワーク公開用のサーバを有する第２の内部ネットワーク（ＤＭＺ：ＤｅＭｉｌｉｔａｒｉｚｅｄ Ｚｏｎｅ）を接続することにより、本発明を適用し、さらにセキュリティを向上することができる。

【００９４】なお、本実施形態では、サービス状態の「使用可」から「使用不可」への状態遷移や「使用不可」から「使用可」への状態遷移、及びサービス情報の登録・削除のために、サーバからの登録情報や有効期限のタイムアウトの情報を用いるとしたが、これに限らず、ＨＧＷ１がサーバに対してポートスキャンを実行し、サーバのオープンされたポートの変化に基づいてサービス状態の遷移やサービス情報の登録・削除を実行するようにしてもよい。同様に、ポートスキャンの代わりにｐｉｎｇを用いてもよい。

【００９５】また、本実施形態では、外部ネットワーク

より内部ネットワークのサーバにアクセスする例を示したが、これに内部ネットワークのべつの機器よりアクセスしてもよい。その場合、現在の公開先に内部ネットワークの機器に対する詳細公開ポリシーを追加する、または、もうひとつ別に公開先のテーブルを持つことで実現できる。これにより、内部からアクセスした場合と外部からアクセスした場合でセキュリティの強度を変えることができ、利便性が増す。

【００９６】なお、あるサーバについてサービス詳細公開ポリシーを作成する際には、宅外の、例えばそのサーバの製造元にアクセスし、そこからサービス詳細公開ポリシーの初期値を取得してもよい。これにより、そのサーバに格納されているサービス詳細公開ポリシーを、製造者はサーバ出荷後も変更することが可能となる。

【００９７】このように、当該ファイアウォール装置では、外部から接続可能なユーザを限定しユーザ認証を確認した後、そのユーザが使用している外部端末のアドレス情報（ＩＡ、ＩＰ）を取得し、そのアドレス情報を基にして通信路を設定している。したがって、内部ネットワークのサービスに対して、外部からアクセス可能なユーザを限定して公開することができ、しかも、上記ユーザがサービス公開を要求する期間のみ通信路を設定することができる。また、上記ユーザが使用する外部端末を変更する、あるいはユーザが使用している外部端末のＩＡが変わっても同様のアクセスが可能である。また、上記ユーザは、通信路を設定する要求をするとき、アクセス可能なサービスを選択的に接続することができ、さらに、同じサービスを内部ネットワーク内で複数のサーバが有していても、上記ユーザは上記サーバを選択的に接続することができる。一方、内部ネットワークのサーバに接続可能なユーザを、そのサーバのサービス毎に設定できるため、内部ネットワークの中で同一のサービスを有する複数のサーバに対して、それぞれの異なった接続可能なユーザを設定することにより、サーバ毎のセキュリティレベルを容易に設定することができる。さらに、内部ネットワークのサーバのアドレス情報（ＬＡ、ＬＰ）が変更された場合、当該ファイアウォール装置は、上記サーバを識別する固定値を認識することにより、上記サーバと変更された上記アドレス情報とを対応させることができるため、アドレス変換時に必要なテーブルの変更を自動的に容易に処理することができる。また、当該ファイアウォール装置は、外部ネットワークに提供可能なサービスに対して有効期限を設けており、上記サービスが有効である時のみ一時的に通信路を設定し、しかも上記サービス専用の通信路であるため、さらにセキュリティの向上を実現できる。

【００９８】なお、本実施形態では、登録しようとするサービスのサービス種別とサーバ識別情報との対がディレクトリ管理機能部３３に未登録であった場合、図４のステップＳ１０９に示すようにサービス基本公開ポリシーに基づいてサービス詳細公開ポリシーを設定するとしたが、他の方法によりサービス詳細公開ポリシーが決定されるようにしても構わない。例えば、サービス詳細公開ポリシーとしてすでに登録されている項目の中から、新たに登録しようとするサービスと同じサービス種別のものの個数を数え、その個数があるしきい値以上である場合にはそれらすでに登録されている項目に基づいてサービス詳細公開ポリシーを設定し、一方、その個数がしきい値未満である場合にはサービス基本公開ポリシーに基づいてサービス詳細公開ポリシーを設定するようにしても構わない。つまり具体的には、図４のステップＳ１０９の代わりに例えば図１４に示す処理が実行されるようにしても構わない。以下、図１４～図１６を参照してより具体的に説明する。

【００９９】今、内部ネットワークにＩＰがＬＡ５であるサーバ２－４が新たに設けられたと仮定する。つまり、ディレクトリ管理機能部３３に図１５に示すようなサービス情報が新たに登録される場合について考える。ディレクトリ管理機能部３３は、図４のステップＳ１０２においてサーバ２－４が提供するサービスが未登録であると判断すると、図１４のステップＳ２０３において、すでにディレクトリ管理機能部３３において管理されているサービス詳細公開ポリシーの中から、新たに登録するサービスに関連する項目を抽出する。次にディレクトリ管理機能部３３はステップＳ２０４において、抽出した項目の数が３以上であるか否かを判断し、３未満である場合には図４のステップＳ１０９と同様の処理によりサービス詳細公開ポリシーを設定する。一方、ステップＳ２０４において項目の数が３以上であると判断された場合には、ステップＳ２０６において、抽出した項目の設定内容に基づいてサービス詳細公開ポリシーを設定する。以上の処理について図１６を参照してより具体的に説明すると、新たに追加されるサーバ２－４のＨＴＴＰサーバの項目については、この項目とサービス種別が一致する項目が２個（図中の項目Ａ，Ｂ）なので、このサーバ２－４のＨＴＴＰサーバの公開先相手・公開条件・公開ポートは、図９に示すサービス基本公開ポリシーに基づいて決定される。一方、サーバ２－４のＦＴＰサーバの項目については、この項目とサービス種別が一致する項目が３個（図中の項目Ｃ～Ｅ）なので、このサーバ２－４のＦＴＰサーバの公開先相手・公開条件・公開ポートは、項目Ｃ～Ｅの設定内容に基づいて決定される。ここでは、項目Ｃ～Ｅに共通の設定がサーバ２－４のＦＴＰサーバの設定に反映される。

【０１００】なお、抽出した項目の設定内容に基づいてサービス詳細公開ポリシーを設定する具体的な方法については種々の方法が考えられる。例えば上記の説明では、サービス詳細公開ポリシーを作成する際、すでに登録されている項目の設定内容の論理積を取ることにより新たなサービスの設定内容を決定したが、これに限ら

ず、例えばすでに登録されている項目の設定内容の論理和や多数決を取ることにより新たなサービスの設定内容を決定しても構わない。これらまたは他の種々の設定方法については下記の種々の実施形態の説明によっても示唆される。

【０１０１】（第２の実施形態）図１７に、本発明の第２の実施形態に係る通信装置１００の構成を示す。通信装置１００は、制御メニュー構成部１１０と、ディレクトリ管理機能部１２０と、制限項目管理部１３０とを備える。制御メニュー構成部１１０は、制御メニュー作成要求受信部１１１と、制御メニュー作成部１１２と、制御メニュー送信部１１３とを含む。ディレクトリ管理機能部１２０は、ネットワーク構成要素検出部１２１と、ネットワーク情報取得部１２２と、ネットワーク情報格納部１２３とを含む。制限項目管理部１３０は、制限項目作成部１３１と、初期制限項目格納部１３２と、個別制限項目格納部１３３と、入力部１３４とを含む。

【０１０２】通信装置１００は、ユーザがネットワークを介して制御端末から被制御端末を制御する際に、予め設定された制限項目に基づいて、その制御を許可したり、あるいは制御を一部制限したり、あるいは制御を禁止したりする機能を有する。より具体的に説明すると、例えば、太郎さんの宅内に設けられたネットワーク（ＩＥＥＥ１３９４バス）に接続されたビデオを被制御端末としてネットワークを介して制御するとき、通信装置１００は、制御を行うのが太郎さんであれば、宅内のネットワークに接続された制御用端末からでも、インターネットに接続された制御用端末としての携帯電話からでもビデオを制御できるようにし、一方、制御を行うのが太郎さんの娘の花子さんであれば、宅内のネットワークに接続された制御用端末からはビデオを制御できるが、携帯電話からは制御できないようにするというように、条件に応じて被制御端末の制御を制限する。

【０１０３】図１７は、一例として、宅外ネットワークとしてのインターネット１６０に接続された例えば携帯電話等の制御端末１４１から、宅内ネットワークとしてのＩＥＥＥ１３９４バス１７０に接続された、それぞれＡＶ／Ｃコマンドを実装した例えばビデオやチューナ等の被制御端末１５１～１５３を制御する場合の構成を示している。

【０１０４】以下、通信装置１００の動作を説明する。ディレクトリ管理機能部１２０は、ネットワークに接続されている機器に関する情報を要素情報として管理している。図１８に、ネットワーク情報格納部１２３で管理される要素情報の一例を示す。図１８において、ＧＵＩＤとは、機器毎にユニークに与えられている６４ビットの識別子である。また、機器カテゴリーとは、機器の種類を示すものである。また、サービス情報とは、機器がネットワークに対して提供できるサービスを示すものである。また、所属ネットワークとは、機器が属するネットワークを示すものである。すなわち、図１８に示す要素情報は、ＩＥＥＥ１３９４バスには、機器として、ネットワークを介して「電源」「録画」「再生」「早送り」「巻き戻し」「停止」の制御が可能な２台のビデオと、ネットワークを介して「電源」「選局」の制御が可能な１台のチューナが接続されていることを示している。

【０１０５】ディレクトリ管理機能部１２０は、通信装置１００に接続されるネットワークに新たな機器が接続されたとき、それを検知して要素情報を更新する機能を有する。以下、この機能について具体的な例で説明する。図１９に、機器１５２、１５３がすでにＩＥＥＥ１３９４バス１７０に接続されている状態で、機器１５１がＩＥＥＥ１３９４バス１７０に新たに接続されたときの動作シーケンスを示す。なお、他の実施形態も含めた以下の説明において、例えば図１７における被制御端末１５１等を、単に機器１５１等として説明しているが、これは、ネットワークに接続されている機器が制御端末となるか被制御端末となるかは、予め決められている必要はなく、例えば機器がＰＣ等であれば、状況に応じて制御端末して利用されたり被制御端末として利用されたりする。よって、制御の主体と客体を意識しない段階では単に機器１５１等としている。ＩＥＥＥ１３９４バス１７０に新たな機器（ここでは機器１５１）が接続されるとバスリセットが発生する。ネットワーク構成要素検出部１２１は、このバスリセットを検出し、バスリセットが発生したことをネットワーク情報取得部１２２に通知する。ネットワーク情報取得部１２２は、この通知を受けると、ＩＥＥＥ１３９４バス１７０に接続されている機器のＧＵＩＤを取得する。ネットワーク情報取得部１２２は、取得したＧＵＩＤをネットワーク情報格納部１２３に通知する。

【０１０６】ネットワーク情報格納部１２３は、すでに格納されている要素情報を参照して、ネットワーク情報取得部１２２から通知されたＧＵＩＤと、バスリセット発生前に接続されていた機器のＧＵＩＤとを比較する。その結果、新たに機器１５１のＧＵＩＤが増えていることが確認されるので、ネットワーク情報格納部１２３は、要素情報を更新すべく、ネットワーク情報取得部１２２に対し、この新たに接続された機器１５１が提供するサービス情報と、機器カテゴリーとを取得するように要求する。ネットワーク情報取得部１２２は、ＡＶ／Ｃコマンドを用いて、機器１５１が提供するサービス情報および機器カテゴリーを示す情報を取得する。

【０１０７】ネットワーク情報取得部１２２は、取得したビデオＡ１５１のサービス情報および機器カテゴリーを示す情報を、ネットワーク情報格納部１２３に通知する。ネットワーク情報格納部１２３は、通知された情報を要素情報に登録することにより、要素情報を更新する。

【０１０８】ユーザが制御端末から被制御端末を制御するには、まず、通信装置１００に対して、被制御端末を制御するための制御メニューを要求する。制御メニュー構成部１１０は、制御端末からの要求に基づいて、制御メニューを構成して制御端末へ送る。図２０に、制御端末に送られた制御メニューの画面表示の一例を示す。ユーザは、この制御メニューに基づいて、例えばビデオＡ１５１の録画を開始するなど、制御端末から被制御端末を制御することができる。制限項目管理部１３０には、種々の条件毎に被制御端末の制御を許可するか禁止するかを規定するための制限項目が、予め設定されて登録されている。図２１に、制限項目管理部１３０において管理されている制限項目の一例を示す。この図２１の例では、被制御端末と、制御を行うユーザと、制御端末のネットワークと、被制御端末のネットワークとの組合せに応じて特定される制御条件毎に、被制御端末の制御を許可するか禁止するかを示す制限情報が設定されている。図２１の例によれば、例えば、「ＩＥＥＥ１３９４」に接続された、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である被制御端末に対して、「太郎」が、「インターネット」に接続された制御端末から制御を行う場合には、制限情報として「アクセス許可（１）」が設定されているため、制御が許可される。一方、「ＩＥＥＥ１３９４」に接続された、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である被制御端末に対して、「花子」が、「インターネット」に接続された制御端末から制御を行う場合には、制限情報として「アクセス不可（０）」が設定されているため、制御が禁止される。制御端末へ送られる制御メニューは、この制限項目管理部１３０が管理している制限項目に基づいて作成され、制御端末から制御することのできる制御内容のみで構成される。これにより、制限項目管理部１３０が管理している制限項目に応じて、制御端末からの被制御端末の制御が制限されることになる。

【０１０９】以下、ユーザが制御端末で制御メニューを取得する際の処理について具体的な例で説明する。図２３に、制御端末１４１で制御メニューを取得するときの動作シーケンスを示す。なお、ここでは、機器１５１がＩＥＥＥ１３９４バス１７０に新たに接続されてから一番最初に制御メニューが要求されたという状況を仮定して説明を行う。ユーザは、制御メニューを取得するために、制御端末１４１を操作して、通信装置１００に対して制御メニュー要求を発行する。制御メニュー作成要求受信部１１１は、この要求を受け、制御メニュー要求を発行したユーザのユーザＩＤおよび制御端末１４１が接続されているネットワークを識別する。ここで、ユーザ識別のための情報取得は、制御端末１４１が制御メニュー要求を発行するまでに行われていればよいが、セキュリティ上、制御端末１４１と通信装置１００とのコネクションが確立した後に制御端末１４１からユーザＩＤおよびパスワードが送付されてユーザ認証が行われるのが望ましい。

【０１１０】制御メニュー作成要求受信部１１１は、ユーザＩＤおよび制御端末のネットワーク情報を制御メニュー作成部１１２に送り、制御メニューの作成を要求する。要求を受けた制御メニュー作成部１１２は、まず、ネットワーク情報格納部１２３に対して、現在ＩＥＥＥ１３９４バス１７０に接続されている機器に関する情報である要素情報を要求する。ここで要求される要素情報は、機器のＧＵＩＤと、機器カテゴリーと、サービス情報と、そのネットワークの種類とからなる。ネットワーク情報格納部１２３は、前述のように管理している要素情報に基づいて、制御メニュー作成部１１２に対して要素情報を通知する。

【０１１１】次に、制御メニュー作成部１１２は、制御メニュー作成要求受信部１１１から受け取ったユーザＩＤおよび制御端末のネットワーク情報と、ネットワーク情報格納部１２３から受け取った要素情報とを制限項目作成部１３１に通知し、これらの情報に応じた制限項目を要求する。

【０１１２】制限項目作成部１３１は、制御メニュー作成部１１２からの制限項目要求を受けると、制御メニュー作成部１１２から通知された「ＧＵＩＤ」と、「ユーザＩＤ」と、「被制御端末のネットワーク」と、「制御端末のネットワーク」とを個別制限項目格納部１３３に送信する。個別制限項目格納部１３３では、前述した図２１に示す制限項目が予め登録されており、制限項目作成部１３１から送信された情報をもとに、それに合致する制限情報を検索し、制限項目作成部１３１に通知する。例えば、要素情報に、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である機器に関する情報が含まれている場合、この機器が現在接続されているネットワーク「ＩＥＥＥ１３９４」と、この機器を制御しようとするユーザのＩＤ「太郎」と、制御端末が接続されているネットワーク「インターネット」との組合せに対して設定されている制限情報を検索する。検索の結果、制限情報として「アクセス許可（１）」が設定されていることが分かる。要素情報に含まれる他のＧＵＩＤで示される機器についても同様の検索を行う。個別制限項目格納部１３３は、こうして得られた制限情報を制限項目作成部１３１に通知する。

【０１１３】なお、図２１に示すのは、新たに接続された機器１５１に関する個別制限項目（図２１に新項目Ａ、Ｂで示す）が後述する処理等によって新たに登録された後の内容を示している。ここでは、これら新項目Ａ、Ｂが、まだ登録されていない状態を仮定して説明を行っているため、この段階における個別制限項目の内容は、図２２に示す内容となっている。

【０１１４】一方、個別制限項目格納部１３３における検索の結果、その条件に合致する制限項目が登録されて

いない場合がある。ネットワークに被制御端末として新たな機器を接続した場合である。また、場合によっては、機器の接続先のネットワークを変更した場合などにもこのような状況が起こり得る。また、太郎に対する登録はされていても、花子に対する登録がまだされていないような場合などにもこのような状況が生じ得る。このような状況が生じたとき、従来では、この新たに接続した機器に対する制限項目をユーザがその都度設定する必要があり、ネットワークに対して十分な知識を持たない者（例えば家族の誰かなど）が勝手に機器をネットワークに接続した場合には、誤った設定が行われて宅外から無制限にアクセスされる可能性があるという問題があることについては前述した通りである。

【０１１５】本実施形態では、個別制限項目格納部１３３における検索の結果、その条件に合致する制限項目が登録されていなかった場合、初期制限項目格納部１３２に予め設定しておいた初期制限項目に基づいて条件に合致した制限情報を取得することにより、ユーザによる設定を必要とすることなく好ましい制限情報が自動的に設定される。より具体的に説明すると、制限項目作成部１３１は、初期制限項目格納部１３２に対し、登録がされていなかった条件について、「ユーザＩＤ」と、「制御端末のネットワーク」と、「被制御端末のネットワーク」とを送信する。初期制限項目格納部１３２は、初期制限項目の中から、この条件に一致する制限情報を検索し、制限項目作成部１３１に対して通知する。図２４に、初期制限項目格納部１３２に登録されている初期制限項目の一例を示す。図２４において、例えば、「ＩＥＥＥ１３９４」に新たな機器が接続され、その後「太郎」が「インターネット」に接続された制御端末から制御メニューを要求した場合、この条件に応じて初期制限項目を検索した結果、この条件に合致した制限情報として「アクセス許可（１）」が設定されているので、これを制限項目作成部１３１に対して通知する。

【０１１６】制限項目作成部１３１は、初期制限項目格納部１３３から通知された制限情報に基づいて、個別制限項目格納部１３３に新たな制限項目を登録する。例えば、ＩＥＥＥ１３９４バス１７０にＧＵＩＤが０ｘ０１２３４５６７８９０１２３４５である被制御端末１５１が新たに接続された後に、太郎がインターネット１６０に接続される制御端末１４１から制御メニューを要求すると、この条件に合致する初期制限項目には「アクセス許可（１）」が設定されているので、個別制限項目格納部１３３に、新たな制限項目として、ＧＵＩＤ「０ｘ０１２３４５６７８９０１２３４５」、ユーザＩＤ「太郎」、制御端末のネットワーク「インターネット」、被制御端末のネットワーク「ＩＥＥＥ１３９４」からなる制御条件に対して制限情報「アクセス許可（１）」を対応付けた制限項目（図２１に示す新項目Ａ）を登録する。

【０１１７】制限項目作成部１３１は、以上の処理により条件に応じた制限情報を取得し、制御メニュー作成部１１２に対して制限項目を通知する。制御メニュー作成部１１２は、ネットワーク情報格納部１２３より通知された被制御端末のネットワーク情報、サービス情報および機器カテゴリーと、制限項目作成部１３１より通知された制限項目に基づいて制御メニューを作成する。制御メニューは、制御端末１４１で実行可能なアプリケーションの形式でもよいが、好ましくは、ＨＴＭＬで記述されたソースであることが望ましい。この場合、制御端末１４１はＨＴＭＬブラウザを装備していれば、機器の制御を行うことが可能となる。さらに、制御メニューで表示される項目と制御コマンドがＣＧＩなどで関連付けられていることが望ましい。

【０１１８】制御メニュー作成部１１２は、作成した制御メニューを制御メニュー送信部１１３に送信する。制御メニュー送信部１１３は、受け取った制御メニューを制御端末（ここでは制御端末１４１）に送信する。制御端末１４１は、制御メニューをブラウザに表示し、ユーザは制御メニューに基づいて操作を行い、被制御端末１５１～１５３の制御を行う。

【０１１９】図２５に示すフローチャートを参照して、制限項目作成部１３１の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部１２３に図１８に示す要素情報が格納されており、初期制限項目格納部１３２に図２４に示す初期制限項目が格納されている状態において、図２１に示す個別制限項目において、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である被制御端末１５１に関する制限項目（図中の新項目Ａ、Ｂ）が未登録である状況、つまり図２２に示す制限項目が登録されている状況、を想定して説明する。

【０１２０】制限項目作成部１３１は、ステップＳ９０１で、制御メニュー作成部１１２より、制限情報を作成する条件として、「ＧＵＩＤ」と「ユーザＩＤ」と「制御端末のネットワーク情報」と「被制御端末のネットワーク情報」を受け取る。ここで受け取る項目は以下の通りである。

【０１２１】ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
被制御端末のネットワーク情報＝ＩＥＥＥ１３９４（以下、単に宅内と称す）
制御端末のネットワーク情報＝インターネット（以下、単に宅外と称す）
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外
ＧＵＩＤ＝０ｘ０１２３４５６７８９２３４５６７

ユーザＩＤ＝太郎
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外

【０１２２】ステップＳ９０２で、上記の条件をもとに、個別制限項目格納部１３３に個別制限項目を送るよう要求する。ステップＳ９０３で、上記の条件に対する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【０１２３】ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎、
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９２３４５６７
ユーザＩＤ＝太郎、
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外
制限情報＝アクセス許可

【０１２４】ステップＳ９０４で、制限情報が存在しない条件が存在するか否かを確認する。存在すればステップＳ９０５に進み、存在しなければステップＳ９０８に進む。ここでは、ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５の条件が、制限情報が存在しない条件にあたる。

【０１２５】ステップＳ９０５で、制限情報が存在しない条件について、初期制限項目格納部１３２に対して、この条件に対応する制限項目を通知するように要求する。ステップＳ９０６で、条件に一致する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【０１２６】ユーザＩＤ＝太郎、
被制御端末のネットワーク情報＝宅内
制御端末のネットワーク情報＝宅外
制限情報＝アクセス許可

【０１２７】ステップＳ９０７で、前述のステップＳ９０６で受け取った制限項目を個別制限項目格納部１３３に登録する。この結果、図２１に新項目Ａで示した個別制限項目が新たに登録される。ステップＳ９０８で、制御条件と制限情報とを対応付けて制御メニュー作成部１１２に通知する。

【０１２８】この後、制御メニュー作成部１１２で作成された制御メニューは、制御メニュー送信部１１３を通じて制御端末１４１に送信される。制御メニュー作成部１１２は、図１８に示されるサービス情報のうち、図２１に示される個別制限項目でアクセスが許可されているものだけを選択し、制御メニューとする。よって、図２０に示すように、ユーザ太郎が操作する制御端末１４１には、ビデオＡ１５１、ビデオＢ１５２、およびチューナ１５３の制御メニューが表示される。

【０１２９】一方、仮に、制御メニューを要求したユーザが花子である場合、上記と同様の処理によって図２１に示す新項目Ｂが新たに登録され、制御メニュー作成部１１２は、図１８に示されるサービス情報のうち、図２１に示される個別制限項目でアクセスが許可されているものだけを選択し、制御メニューとするのであるが、ユーザ花子についてはすべての制限項目で、インターネット１６０を通じたアクセスが不可に設定されているため、図２６に示すように、ユーザ花子が操作する制御端末１４１には、制御可能な制御項目は表示されない。

【０１３０】なお、個別制限項目格納部１３３に格納されている個別制限項目は、入力部１３４よりユーザが設定することができる。これは、制限項目作成部１３１で作成されて登録された制限項目についても同様である。また、初期制限項目格納部１３２に格納されている初期制限項目についても、入力部１３４よりユーザが設定することができる。

【０１３１】なお、本実施形態では、宅外からのアクセスとして、インターネット１６０に接続されている制御端末１４１より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のＩＥＥＥ１３９４バス１７０またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【０１３２】また、本実施形態では、ユーザＩＤとして「太郎」を例にあげたが、これはユーザを識別するＩＤの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」や「花子」といった個人を対象としたユーザＩＤを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【０１３３】また、本実施形態では、被制御端末が接続されるネットワークとしてＩＥＥＥ１３９４バス１７０、制御端末が接続されるネットワークとしてインターネット１６０を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ＥＣＨＯＮＥＴやＢｌｕｅｔｏｏｔｈなどが挙げられる。

【０１３４】また、本実施形態では、２つのネットワークが通信装置１００に接続される例を示したが、これに限らず、通信装置１００に接続されるネットワークの数は１つまたは３以上であっても構わない。

【０１３５】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、２つの機器が連携して提供されるサービス、例え

ば、ビデオのダビングや通信路設定などであっても構わない。

【０１３６】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリーや、サービス情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【０１３７】また、本実施形態では、被制御端末として、ビデオＡ、ビデオＢおよびチューナを例に挙げたが、チューナが通信装置を通じてビデオＡを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【０１３８】また、本実施形態では、機器カテゴリーの分類項目としてビデオやチューナを使用したが、ＡＶ機器や空調機器など他の分類を行っても構わない。

【０１３９】また、本実施形態では、ネットワーク情報格納部１２３に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部１１２から要素情報を要求された時点で、ネットワーク情報取得部１２２が要素情報を取得して制御メニュー作成部１１２に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【０１４０】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が短くなるという利点がある。

【０１４１】以上のように、第２の実施形態によれば、対応する個別制限項目が存在しない場合、初期制限項目を用いてアクセス制限を行うため、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【０１４２】また、制御機器が接続されるネットワークの種類に応じてアクセス制限を設定しているため、例えばインターネットのように不特定多数が利用するネットワークであればアクセスを不可とし、ＩＥＥＥ１３９４バスのような宅内のネットワークであればアクセスを許可するというように、利便性と安全性を両立した制限が可能となる。

【０１４３】（第３の実施形態）以下、本発明の第３の実施形態に係る通信装置について、図面を参照しながら説明する。図２７に、本実施形態に係る通信装置１０００と、それに接続されるネットワークおよび制御端末、被制御端末とを示す。図２７において、通信装置１０００は、制御メニュー構成部１１０と、ディレクトリ管理機能部１２０と、制限項目管理部１０３０とを含む。制御メニュー構成部１１０は、制御メニュー作成要求受信部１１１と、制御メニュー作成部１１２と、制御メニュー送信部１１３とを含む。ディレクトリ管理機能部１２０は、ネットワーク構成要素検出部１２１と、ネットワーク情報取得部１２２と、ネットワーク情報格納部１２３とを含む。制限項目管理部１０３０は、制限項目作成部１０３１と、個別制限項目格納部１３３と、入力部１３４とを含む。通信装置１０００は、インターネット１６０と、ＩＥＥＥ１３９４バス１７０に接続され、それらネットワークには、それぞれ制御端末１４１（例えば、携帯電話）およびＡＶ／Ｃコマンドを実装した被制御端末１５１、１５２、１０５４（例えば、ビデオＡ、ビデオＢ、ビデオＣ）が接続される。なお、図２７において、図１７と同一の構成には同一の参照符号を付し、その説明を省略する。

【０１４４】以下、通信装置１０００の動作を、特に第２の実施形態に係る通信装置１００との相違点を中心に説明する。ここでは、例として、機器１５１が新たに接続され、機器１５１、１５２、１０５４をユーザ（太郎）がインターネット１６０に接続された機器１４１から制御するために制御メニューを要求する場合について説明を行う。

【０１４５】図２８に、機器１５１がＩＥＥＥ１３９４バス１７０に接続されたときの動作シーケンスを示す。図２８に示すように、第２の実施形態と同様の動作により、ネットワーク情報格納部１２３に要素情報が更新され登録される。図２９に、ネットワーク情報格納部１２３に格納される要素情報の一例を示す。なお、図２９に示す要素情報には、図１８に示した「被制御端末のネットワーク」の情報が含まれていないが、これは、制限情報を設定する制限項目の条件として「被制御端末のネットワーク」についての情報が含まれないためである。

【０１４６】制御メニュー構成部１１０は、第２の実施形態と同様に、制御端末１４１からの要求に応じて制御メニューを作成する。このとき、制限項目管理部１０３０に対して、制限項目を要求する。制限項目管理部１０３０では、制御メニュー作成部１１２から通知される条件に応じた制限項目を制御メニュー作成部１１２に対して返すのであるが、第２の実施形態とは異なり、初期制限項目格納部を含んでいない。その代わり、個別制限項目格納部１３３に条件に合致した制限項目が存在しなかった場合には、すでに個別制限項目格納部１３３に格納されている制限項目に基づいて、この制限項目がない条件に対する好ましい制限情報を自動的に判断して決定する。以下、その具体的な動作について説明する。

【０１４７】図３０に、インターネットに接続された携帯電話１４１を使用して、ユーザＩＤとして太郎で登録

されているユーザが被制御端末１５１を制御するための制御メニューを取得する際の動作シーケンスを示す。制御端末１４１で制御メニューを要求してから制限項目作成部１０３１に制限項目要求が発行されるまでの動作については、第２の実施形態と同様であるので説明を省略する。

【０１４８】制限項目作成部１０３１は、受け取った条件を個別制限項目格納部１３３に送り、制限項目の発行を要求する。個別制限項目格納部１３３は、受け取った条件に合致する制限情報を検索して制限項目作成部１０３１に通知する。図３１に、個別制限項目格納部１３３に格納される制限項目の一例を示す。

【０１４９】なお、図３１に示すのは、新たに接続された機器１５１に関する個別制限項目（図３１に新項目Ａ、Ｂで示す）が後述する処理によって新たに登録された後の内容を示している。ここでは、これら新項目Ａ、Ｂが、まだ登録されていない状態を仮定して説明を行っている。

【０１５０】ここで、被制御端末１５１は、新たにＩＥＥＥ１３９４バス１７０に追加された機器であるため、個別制限項目格納部１３３には被制御端末１５１のＧＵＩＤは登録されていない。制限項目作成部１０３１は、ＧＵＩＤの一致する制限項目が個別制限項目格納部１３３に登録されていなかった場合、他の機器に適用するために登録されている制限項目の中から、この条件と「ユーザＩＤ」、「機器カテゴリー」、および「制御端末のネットワーク情報」が一致する制限項目の検索を個別制限項目格納部１３３に対して要求する。個別制限項目格納部１３３は、この要求を受けて制限情報を検索し、その結果を、制限項目作成部１０３１に通知する。制限項目作成部１０３１は、これらの制限情報を元に、登録されていない条件に対する制限情報を決定する。具体的には、制限情報のアクセス許可を１、アクセス不可を０とし、取得した制限情報で論理積をとることにより決定する。このように論理積を取ることで、設定されたすべての制限情報がアクセス許可でなければ、新たに接続された機器およびサービスもアクセス可能とはならず、不用意にアクセスを許可することがない。

【０１５１】こうして新たに作成された制限項目は、第２の実施形態と同様に個別制限項目格納部１３３に登録される。制限項目作成部１０３１は、要求された制限項目を制御メニュー作成部１１２に通知し、制御メニュー作成部１１２は、通知に基づいて制御メニューを作成する。この制御メニューは、制御メニュー送信部１１３を通じて制御端末１４１に送信される。制御端末１４１は、制御メニューをブラウザで表示し、ユーザは制御メニューに基づいて制御端末１４１を操作して被制御端末１５１の操作を行う。

【０１５２】図３２に示すフローチャートを参照して、制限項目作成部１０３１の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部１２３に図２９に示す要素情報が格納されており、図３１に示す個別制限項目において、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である被制御端末１５１に関する制限項目（図中の新項目Ａ、Ｂ）が未登録である状況を想定して説明する。ただし、図３２において、図２５に示すフローと同一の処理ステップについては同一の参照符号を付し、説明を省略する。

【０１５３】制限項目作成部１０３１は、制御メニュー作成部１１２から受け取った条件を個別制限項目格納部１３３に通知し、条件に応じた制限情報を個別制限項目格納部１３３より取得する。ここで取得する項目は以下の通りである。

【０１５４】ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
機器カテゴリー＝ビデオ
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
機器カテゴリー＝ビデオ
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９２３４５６７
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
機器カテゴリー＝ビデオ
制限情報＝アクセス許可

【０１５５】ステップＳ９０４で、制限情報が存在しない条件があるか確認する。存在すればステップＳ１６０９に進み、存在しなければステップＳ９０８に進む。ここでは、ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５に関する条件がこれにあたる。ステップＳ１６０９で、個別制限項目格納部１３３に対して、制限情報が存在しない条件について、ＧＵＩＤ以外の条件に合致する制限項目を通知するように要求する。ステップＳ１６１０で、前のステップＳ１６０９で要求した制限項目を受け取る。ここで受け取る項目は以下の通りである。

【０１５６】ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
機器カテゴリー＝ビデオ
制限項目＝アクセス許可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
機器カテゴリー＝ビデオ
制限項目＝アクセス許可

【０１５７】ステップＳ１６１１で、これら制限項目の制限情報に対して論理積を取り、それをこの制限項目が

登録されていない条件に対する制限情報とする。こうして作成される制限項目は以下の通りである。

【０１５８】ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５

ユーザＩＤ＝太郎

制御端末のネットワーク情報＝インターネット

機器カテゴリー＝ビデオ

制限項目＝アクセス許可

【０１５９】ステップＳ９０７で、新たに作成した制限項目を個別制限項目格納部１３３に登録する。この結果、図３１に新項目Ａで示した個別制限項目が新たに登録される。ステップＳ９０８で、要求に応じた制限項目を制御メニュー作成部１１２に通知する。制御メニュー作成部１１２は、図２９に示されるサービス情報のうち、図３１に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末１４１では図３３に示すように、ビデオＡ１５１、ビデオＢ１５２、ビデオＣ１０５.4の制御メニューが表示される。

【０１６０】一方、ユーザ（花子）が制御端末１４１より制御メニューを要求した場合、上記と同様の処理によって図３１に示す新項目Ｂが新たに登録され、制御メニュー作成部１１２は、太郎の場合と同様に、図２９に示されるサービス情報のうち、図３１に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末１４１では図３４に示すように、ビデオＢ１５２の制御メニューのみが表示される。

【０１６１】なお、個別制限項目格納部１３３に格納されている個別制限項目は、入力部１３４よりユーザが設定することができる。これは、制限項目作成部１０３１で作成されて登録された制限項目についても同様である。

【０１６２】なお、本実施形態では、宅外からのアクセスとして、インターネット１６０に接続されている制御端末１４１より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のＩＥＥＥ１３９４バス１７０またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【０１６３】また、本実施形態では、ユーザＩＤとして「太郎」を例にあげたが、これはユーザを識別するＩＤの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」や「花子」といった個人を対象としたユーザＩＤを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【０１６４】また、本実施形態では、被制御端末が接続されるネットワークとしてＩＥＥＥ１３９４バス１７０、制御端末が接続されるネットワークとしてインターネット１６０を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ＥＣＨＯＮＥＴやＢｌｕｅｔｏｏｔｈなどが挙げられる。

【０１６５】また、本実施形態では、２つのネットワークが通信装置１０００に接続される例を示したが、これに限らず、通信装置１０００に接続されるネットワークの数は１つまたは３以上であっても構わない。

【０１６６】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、２つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

【０１６７】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、サービス情報や、被制御端末が属するネットワークの情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【０１６８】また、本実施形態では、被制御端末として、ビデオＡ、ビデオＢ、およびビデオＣを例に挙げたが、ビデオＡが通信装置を通じてビデオＢを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【０１６９】また、本実施形態では、機器カテゴリーの分類項目としてビデオを使用したが、ＡＶ機器や空調機器など他の分類を行っても構わない。

【０１７０】また、本実施形態では、制限項目を作成する際、個別制限項目をもとに制限情報の論理積を取ることにより制限項目を作成したが、これに限らず、例えば制限情報の論理和や多数決を取って作成しても構わない。

【０１７１】また、本実施形態では、ネットワーク情報格納部１２３に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部１１２から要素情報を要求された時点で、ネットワーク情報取得部１２２が要素情報を取得して制御メニュー作成部１１２に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【０１７２】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が

納部１３３は、その結果を制限項目作成部１８３１に通知する。制限項目作成部１８３１は、通知された制限項目の数を数え、その結果、その数が３個より少ない場合、図３８に示すように、第２の実施形態と同様の処理を行う。すなわち、制限項目作成部１８３１は、初期制限項目格納部１３２に対し、ＧＵＩＤを除いた条件を送信し、初期制限項目格納部１３２は、予め登録されている初期制限項目の中から、この条件に一致する制限項目を検索し、制限項目作成部１８３１に対して通知する。図４０に、初期制限項目格納部１３２に格納されている初期制限項目の一例を示す。制限項目作成部１８３１は、通知された制限情報を条件と対応付けて、制限項目として個別制限項目格納部１３３に登録するとともに、制御メニュー作成部１１２に対して、要求された制限項目を通知する。

【０１８３】一方、制限項目作成部１８３１において、通知された制限項目の数を数えた結果、その数が３個以上だった場合には、図４１に示すように、第３の実施形態と同様の処理を行う。すなわち、制限項目作成部１８３１は、個別制限項目格納部１３３より受け取った、他の機器に適用するために登録されている制限項目に基づいて制限情報を決定し、制限項目を作成する。具体的には、制限情報のアクセス許可を１、アクセス不可を０とし、取得した制限情報で論理積をとって、制限情報を決定する。このように論理積を取ることで、設定されたすべての制限情報がアクセス許可でなければ、新たに接続された機器およびサービスもアクセス可能とはならず、不用意にアクセスを許可することがない。制限項目作成部１８３１は、決定した制限情報を条件と対応付けて、制限項目として個別制限項目格納部１３３に登録するとともに、制御メニュー作成部１１２に対して、要求された制限項目を通知する。

【０１８４】制御メニュー作成部１１２に対して、要求された制限項目を通知した以降の動作については、第２の実施形態および第３の実施形態と同様であるため、説明を省略する。

【０１８５】図４２に示すフローチャートを参照して、制限項目作成部１８３１の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部１２３に図３７に示す要素情報が格納されており、初期制限項目格納部１３２に図４０に示す初期制限項目が格納されており、図３９に示す個別制限項目において、ＧＵＩＤが「０ｘ０１２３４５６７８９０１２３４５」である被制御端末１５１に関する制限項目（図中の新項目Ａ～Ｆ）を除く制限項目が登録されている状況を想定して説明する。ただし、図４２において、図２５または図３２に示すフローと同一の処理ステップについては同一の参照符号を付し、説明を省略する。

【０１８６】制限項目作成部１８３１は、ステップＳ９０１からステップＳ９０３において、制御メニュー作成部１１２から受け取った条件を個別制限項目格納部１３３に通知し、個別制限項目格納部１３３より条件に応じた制限情報を取得する。ここで取得する項目は以下の通りである。

【０１８７】ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝電源
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝録画
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝再生
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝早送り
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝巻き戻し
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝停止
制限情報＝
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝電源
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝録画
制限情報＝アクセス不可
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝再生
制限情報＝アクセス許可

短くなるという利点がある。

【０１７３】以上のように、第３の実施形態によれば、対応する個別制限項目が存在しない場合、すでに登録されている個別制限項目より、制限情報の論理和や論理積、多数決を取ることで、対応する個別制限項目を作成するので、初期制限項目を保持する必要が無く、必要とするメモリの容量を低減することができる。また、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【０１７４】また、機器カテゴリーに応じてアクセス制限を設定しているため、例えばビデオなどのＡＶ機器についてはセキュリティを甘くし、空調機器などについてはセキュリティを高めるというように、利便性と安全性を両立した制御が可能となる。

【０１７５】（第４の実施形態）以下、本発明の第４の実施形態に係る通信装置について、図面を参照しながら説明する。図３５に、本実施形態に係る通信装置１８００と、それに接続されるネットワークおよび制御端末、被制御端末とを示す。図３５において、通信装置１８００は、制御メニュー作成部１１０と、ディレクトリ管理機能部１２０と、制限項目管理部１８３０とを含む。制御メニュー構成部１１０は、制御メニュー作成要求受信部１１１と、制御メニュー作成部１１２と、制御メニュー送信部１１３とを含む。ディレクトリ管理機能部１２０は、ネットワーク構成要素検出部１２１と、ネットワーク情報取得部１２２と、ネットワーク情報格納部１２３とを含む。制限項目管理部１８３０は、制限項目作成部１８３１と、初期制限項目格納部１３２と、個別制限項目格納部１３３と、入力部１３４とを含む。通信装置１８００は、インターネット１６０と、ＩＥＥＥ１３９４バス１７０に接続され、それらネットワークには、それぞれ制御端末１４１（例えば、携帯電話）およびＡＶ／Ｃコマンドを実装した被制御端末１５１～１５３（例えば、ビデオＡ、ビデオＢ、チューナ）が接続される。なお、図３５において、図１７と同一の構成には同一の参照符号を付し、その説明を省略する。

【０１７６】以下、通信装置１８００の動作を、特に第２の実施形態に係る通信装置１００および第３の実施形態に係る通信装置１０００との相違点を中心に説明する。ここでは、例として、機器１５１が新たに接続され、機器１５１、１５２、１０５４をユーザ（太郎）がインターネット１６０に接続された機器１４１から制御するために制御メニューを要求する場合について説明を行う。

【０１７７】図３６に、機器１５１がＩＥＥＥ１３９４バス１７０に接続されたときの動作シーケンスを示す。図３６に示すように、第２の実施形態と同様の動作により、ネットワーク情報格納部１２３に要素情報が更新され登録される。図３７に、ネットワーク情報格納部１２３に格納される要素情報の一例を示す。

【０１７８】制御メニュー構成部１１０は、第２の実施形態と同様に、制御端末１４１からの要求に応じて制御メニューを作成する。このとき、制限項目管理部１８３０に対して、制限項目を要求する。制限項目管理部１８３０では、制御メニュー作成部１１２から通知される条件に応じた制限項目を制御メニュー作成部１１２に対して返すのであるが、個別制限項目格納部１３３に条件に合致した制限項目が存在しなかった場合に、すでに個別制限項目格納部１３３に格納されている制限項目のうち、この条件に対応する制限項目を作成するのに必要な制限項目が一定数以上存在するときには、第３の実施形態と同様に、これら制限項目に基づいて条件に合致した制限項目を作成する。一方、条件に対応する制限項目を作成するのに必要な制限項目が一定数以上存在していないときには、第２の実施形態と同様に、初期制限項目格納部１３２に格納されている初期制限項目に基づいてこの条件に対応する制限項目を作成する。以下、その具体的な動作について説明する。

【０１７９】図３８に、インターネットに接続された携帯電話１４１を使用して、ユーザＩＤとして太郎で登録されているユーザが被制御端末１５１を制御するための制御メニューを取得する際の動作シーケンスを示す。制御端末１４１で制御メニューを要求してから制限項目作成部１８３１に制限項目要求が発行されるまでの動作については、第２の実施形態および第３の実施形態と同様であるので説明を省略する。

【０１８０】制限項目作成部１８３１は、受け取った条件を個別制限項目格納部１３３に送り、制限項目の発行を要求する。個別制限項目格納部１３３は、受け取った条件に合致する制限情報を検索して制限項目作成部１８３１に通知する。図３９に、個別制限項目格納部１３３に格納されている制限項目の一例を示す。

【０１８１】なお、図３９に示すのは、新たに接続された機器１５１に関する個別制限項目（図３９に新項目Ａ～Ｆで示す）が後述する処理によって新たに登録された後の内容を示している。ここでは、これら新項目Ａ～Ｆが、まだ登録されていない状態を仮定して説明を行っている。なお、図３９では、制限項目の条件として、サービス情報による条件が含まれている場合を示している。

【０１８２】ここで、被制御端末１５１は、新たにＩＥＥＥ１３９４バス１７０に追加された機器であるため、個別制限項目格納部１３３には被制御端末１５１のＧＵＩＤは登録されていない。制限項目作成部１８３１は、ＧＵＩＤの一致する制限項目が個別制限項目格納部１３３に登録されていなかった場合、他の機器に適用するために登録されている制限項目の中から、この条件と「ユーザＩＤ」、「機器カテゴリー」、および「制御端末のネットワーク情報」が一致する制限項目の検索を個別制限項目格納部１３３に対して要求する。個別制限項目格

ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝早送り
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝巻き戻し
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９１２３４５６
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝停止
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９２３４５６７
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝電源
制限情報＝アクセス許可
ＧＵＩＤ＝０ｘ０１２３４５６７８９２３４５６７
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝選局
制限情報＝アクセス許可

【０１８８】ステップＳ９０４で、制限情報が存在しない条件があるか確認する。存在すればステップＳ１６０９に進み、存在しなければステップＳ９０８に進む。ここでは、ＧＵＩＤ＝０ｘ０１２３４５６７８９０１２３４５の条件がこれにあたる。ステップＳ１６０９で、個別制限項目格納部１３３に対して、制限情報が存在しない条件について、ＧＵＩＤ以外の条件に合致する制限項目を通知するように要求する。ステップＳ１６１０で、前のステップＳ１６０９で要求した制限項目を受け取る。ここで受け取る項目は以下の通りである。

【０１８９】ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝電源
制限情報＝アクセス許可
個数＝２
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝録画
制限情報＝アクセス不可
個数＝１
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝再生
制限情報＝アクセス許可
個数＝１

ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝早送り
制限情報＝アクセス許可
個数＝１
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝巻き戻し
制限情報＝アクセス許可
個数＝１
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝停止
制限情報＝アクセス許可
個数＝１

【０１９０】ステップＳ２６１２で、受け取った制限項目の数が閾値で定めた３以上であるか否かを判定し、３より少ない場合はステップＳ９０５およびステップＳ９０６を実行し、３以上の場合はステップＳ１６１１に進む。この例では、個数は１または２であるので、ステップＳ９０５に進む。

【０１９１】ステップＳ９０５で、制限情報が存在しない条件について、初期制限項目格納部１３２に対して、この条件に対応する制限項目を通知するように要求する。ステップＳ９０６で、前のステップＳ９０５の要求に対する条件に一致する制限項目を受け取る。ここで受け取る項目は以下の通りである。

【０１９２】ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝電源
制限情報＝アクセス許可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝録画
制限情報＝アクセス不可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝再生
制限情報＝アクセス許可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝早送り
制限情報＝アクセス許可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝巻き戻し
制限情報＝アクセス許可
ユーザＩＤ＝太郎
制御端末のネットワーク情報＝インターネット
サービス情報＝停止

制限情報＝アクセス許可

【０１９３】一方、ステップＳ１６１１では、前のステップＳ１６１０で受け取った制限情報に対して、論理積を取り、それをこのＧＵＩＤである機器のサービスに対する制限情報とする。

【０１９４】ステップＳ９０７で、ステップＳ９０６で受け取りまたはステップＳ１６１０で作成した制限項目を、個別制限項目格納部１３３に登録する。この結果、図３９に新項目Ａ～Ｆで示した個別制限項目が新たに登録される。ステップＳ９０８で、条件と制限情報を対応付けて、制御メニュー作成部１１２に通知する。制御メニュー作成部１１２は、図３７に示されるサービス情報のうち、図３９に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末１４１では図４３に示すように、ビデオＡ１５１、ビデオＢ１５２、チューナ１５３の制御メニューが表示される。

【０１９５】なお、本実施形態では、閾値は３を使用したが、これに限らず、他の値、例えば１や２、または４以上の値を使用しても構わない。

【０１９６】なお、個別制限項目格納部１３３に格納されている個別制限項目は、入力部１３４よりユーザが設定することができる。これは、制限項目作成部１８３１で作成されて登録された制限項目についても同様である。また、初期制限項目格納部１３２に格納されている初期制限項目についても、入力部１３４よりユーザが設定することができる。

【０１９７】なお、本実施形態では、宅外からのアクセスとして、インターネット１６０に接続されている制御端末１４１より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のＩＥＥＥ１３９４バス１７０またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【０１９８】また、本実施形態では、ユーザＩＤとして「太郎」を例にあげたが、これはユーザを識別するＩＤの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」という個人を対象としたユーザＩＤを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【０１９９】また、本実施形態では、被制御端末が接続されるネットワークとしてＩＥＥＥ１３９４バス１７０、制御端末が接続されるネットワークとしてインターネット１６０を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ＥＣＨＯＮＥＴやＢｌｕｅｔｏｏｔｈなどが挙げられる。

【０２００】また、本実施形態では、２つのネットワークが通信装置１８００に接続される例を示したが、これに限らず、通信装置１８００に接続されるネットワークの数は１つまたは３以上であっても構わない。

【０２０１】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、２つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

【０２０２】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリーや、被制御端末が属するネットワークの情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【０２０３】また、本実施形態では、被制御端末として、ビデオＡ、ビデオＢおよびチューナを例に挙げたが、チューナが通信装置を通じてビデオＡを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【０２０４】また、本実施形態では、機器カテゴリーの分類項目としてビデオやチューナを使用したが、ＡＶ機器や空調機器など他の分類を行っても構わない。

【０２０５】また、本実施形態では、制限項目を作成する際、個別制限項目をもとに制限情報の論理積を取ることにより制限項目を作成したが、これに限らず、例えば制限情報の論理和や多数決を取って作成しても構わない。

【０２０６】また、本実施形態では、ネットワーク情報格納部１２３に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部１１２から要素情報を要求された時点で、ネットワーク情報取得部１２２が要素情報を取得して制御メニュー作成部１１２に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【０２０７】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が短くなるという利点がある。

【０２０８】以上のように、第４の実施形態によれば、対応する個別制限項目が存在しない場合において、すでに登録されている個別制限項目が少ない場合は、初期制限項目を用いてアクセス制限を行い、一方、登録されている個別制限項目が多い場合は、すでに登録されている

個別制限項目より、論理和や論理積や多数決を取ることで対応する個別制限項目を作成するので、参照する個別制限項目が少ないために発生するアクセス制限の偏りを防ぎながら、実際に設定されているアクセス制限の傾向を反映することが可能となる。さらに、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【０２０９】また、サービスの種類に応じてアクセス制限の設定を行っているため、例えば再生は可能とするが、録画は禁止するというように、利便性と安全性を両立した制御が可能となる。

【０２１０】（第５の実施形態）以下、本発明の第５の実施形態に係る通信装置について、図面を参照しながら説明する。図４４に、本実施形態に係る通信装置２７００と、それに接続されるネットワークおよび制御端末、被制御端末とを示す。図４４において、通信装置２７００は、制御コマンド中継部２７１０と、ディレクトリ管理機能部２７２０と、制限項目管理部１３０とを備える。制御コマンド中継部２７１０は、制御コマンド送受信部２７１３と、制御コマンド判定部２７１２とを含む。ディレクトリ管理機能部２７２０は、ネットワーク構成要素検出部１２１と、ネットワーク情報取得部１２２と、ネットワーク情報格納部１２３と、インターネットプロトコルをＩＥＥＥ１３９４プロトコルに変換するＩＥＥＥ１３９４プロトコル変換部２７２４と、インターネットプロトコルをＥＣＨＯＮＥＴプロトコルに変換するＥＣＨＯＮＥＴプロトコル変換部２７２５とを含む。制限項目管理部１３０は、制限項目作成部１３１と、初期制限項目格納部１３２と、個別制限項目格納部１３３と、入力部１３４とを含む。

【０２１１】通信装置２７００は、インターネット１６０、ＩＰネットワーク２７８０、ＩＥＥＥ１３９４バス１７０、およびＥＣＨＯＮＥＴ２７９０の各ネットワークに接続される。インターネット１６０には、制御端末１４１（例えば携帯電話）が接続され、ＩＰネットワーク２７８０には、被制御端末２７５５（例えばＰＣ）が接続され、ＩＥＥＥ１３９４バス１７０には、ＡＶ／Ｃコマンドを実装した機器である被制御端末２７５６（例えばビデオ）が接続され、ＩＣＨＯＮＥＴ２７９０には、被制御端末２７５７（例えばエアコン）が接続されている。ここで、インターネット１６０を宅外ネットワーク、その他のネットワーク２７８０、１７０、２７９０を宅内のネットワークとする。

【０２１２】なお、図４４において、図１７と同一の構成には同一の参照符号を付し、説明を省略する。以下、通信装置２７００の動作を説明する。この動作を示す例として、宅外のインターネット１６０に接続された機器１４１を利用して、宅内の機器２７５７を初めて使用する場合について説明を行う。

【０２１３】図４５に、ネットワーク情報格納部１２３が、サービスの制御メニューを作成するために機器のサービス情報を取得する際のシーケンスを示す。

【０２１４】ネットワーク情報格納部１２３は、ネットワーク情報取得部１２２に対して、宅内ネットワークに接続されている機器のサービス情報を収集するように要求する。ネットワーク情報取得部１２２は、サービス情報取得要求を受け取ると、各ネットワークに接続されている被制御端末（エアコン）２７５７、被制御端末（ビデオ）２７５６、被制御端末（ＰＣ）２７５５に対し、サービス情報を通知するように要求する。このとき、ビデオ２７５６およびエアコン２７５７は、接続されているネットワークが異なるため、それぞれＩＥＥＥ１３９４プロトコル変換部２７２４およびＥＣＨＯＮＥＴプロトコル変換部２７２５を通してプロトコル変換を行うことで、要求を発行する。

【０２１５】エアコン２７５７、ビデオ２７５６、およびＰＣ２７５５は、サービス情報取得要求に対し、その機器がネットワークに提供できるサービスの制御コマンドを、ネットワーク情報取得部１２２に送信する。このとき、あわせて、予め登録されてある機器の名前と機器カテゴリーとサービス名も通知する。機器カテゴリーは、ＰＣやＡＶ機器や空調機器などといった機器の種類を示す。機器の名前およびサービス名は、ユーザがそのサービスを識別するために使用するためのものであり、機器の名前としては、例えばＰＣやビデオなどであり、サービス名としては、制御コマンドの動作を示す名前、例えば録画や再生などが望ましい。

【０２１６】ネットワーク情報取得部１２２は、各機器から収集したサービス情報等の情報をネットワーク情報格納部１２３に登録する。図４６に、ネットワーク情報格納部１２３に格納される情報の一例を示す。ネットワーク情報格納部１２３は、その登録された情報に基づいて制御メニューを作成する。

【０２１７】図４７に、宅外のインターネット１６０に接続された携帯電話１４１を使用して、通信装置２７００より制御メニューを取得し、その制御メニューにある制御コマンドを発行して宅内ネットワーク２７９０のエアコン２７５７を制御するときの動作シーケンスを示す。ユーザは、携帯電話１４１を操作して、通信装置２７００が保持している制御メニューを送信するよう通信装置２７００に対して要求する。メニュー要求を受けた通信装置２７００の制御コマンド送受信部２７１３は、ネットワーク情報格納部１２３が保持している制御メニューを要求し、これを受けて、ネットワーク情報格納部１２３は、制御コマンド送受信部２７１３に対し制御メニューを送信する。

【０２１８】制御コマンド送受信部２７１３は、制御端末１４１に対し、制御メニューを送信する。制御メニューは、制御端末１４１で実行可能なアプリケーションの

形式でもよいが、好ましくは、ＨＴＭＬで記述されたソースであることが望ましい。この場合、制御端末１４１は、ＨＴＭＬブラウザを装備していれば、機器の制御を行うことが可能となる。また、制御メニューで表示される項目と制御コマンドとがＣＧＩなどで関連付けられていることが望ましい。

【０２１９】次に、ユーザは、制御メニューに基づいて制御端末１４１を操作し、希望する制御コマンドを発行する。コマンド発行時には、制御対象の機器識別子の情報もあわせて送られる。ここで、機器識別子は、宅内ネットワークに接続されている機器を、通信装置２７００が一意に識別するためのものであり、ネットワーク情報格納部１２３が、各ネットワークに固有のアドレス体系から作成するものである。

【０２２０】制御端末１４１から発行された制御コマンドは、制御コマンド送受信部２７１３で受信され、制御コマンド送受信部２７１３は、受信したコマンドおよび機器識別子を、制御コマンド判定部２７１２に転送する。このとき、あわせて、制御端末１４１が属するネットワーク情報も通知する。制御コマンド判定部２７１２は、ネットワーク情報格納部１２３に対し、機器識別子に対応する機器カテゴリーを通知するように要求する。ネットワーク情報格納部１２３は、この要求を受けて、機器カテゴリーを通知する。

【０２２１】次に、制御コマンド判定部２７１２は、制限項目作成部１３１に対し、制御端末１４１から受信した制御コマンドに対する制限情報を通知するように要求する。このとき、制限情報を検索するための条件として、機器識別子と、制御端末のネットワーク情報と、機器カテゴリーと、制御コマンドとをあわせて送信する。ここで、制限情報は、制御コマンドを使用することができるか否を示す。

【０２２２】制限項目作成部１３１は、受け取った機器識別子および制御端末のネットワーク情報をあわせて、個別制限項目格納部１３３に制限項目要求を発行する。図４８に、個別制限項目格納部１３３に格納されている制限項目の一例を示す。ただし、図４８に示すのは、新たに接続された機器２５７５に関する個別制限項目（図４８に新項目Ａで示す）が後述する処理によって新たに登録された後の内容を示している。ここでは、この新項目Ａが、まだ登録されていない状態を仮定して説明を行っている。個別制限項目格納部１３３は、受け取った機器識別子と制御端末のネットワーク情報に合致する制限項目を検索し、制限項目作成部１３１に通知する。制限項目作成部１３１が、個別制限項目格納部１３３に条件に合致する制限項目がないと判断した場合、制限項目作成部１３１は、初期制限項目格納部１３２に対し、制御端末のネットワーク情報と、機器カテゴリーとを送信する。初期制限項目格納部１３２は、初期制限項目の中から、この条件に一致する制限項目を検索し、制限項目作成部１３１に対して通知する。図４９に、初期制限項目格納部１３２に格納される初期制限項目の一例を示す。ここで、エアコン２７５７は、宅外ネットワークから初めて制御されるため、エアコン２７５７の機器識別子は個別制限項目格納部１３３には登録されていない。よって、制限項目作成部１３１は、初期制限項目格納部１３２から条件に合致する制限項目を取得することになる。制限項目作成部１３１は、通知された初期制限項目と、機器識別子と、制御端末のネットワーク情報とを対応づけて、個別制限項目格納部１３３に登録する。

【０２２３】制限項目作成部１３１は、制御コマンド判定部２７１２に対して、制限項目と、機器識別子と、制御端末のネットワーク情報とを通知する。制御コマンド判定部２７１２は、通知された制限項目に基づいて、受信した制御コマンドを発行してもよいか否か判定する。制限項目においてアクセス許可になっている場合は、制御コマンド判定部２７１２は、受信した制御コマンドをＥＣＨＯＮＥＴプロトコル変換部２７２５に発行する。ＥＣＨＯＮＥＴプロトコル変換部２７２５は、ＥＣＨＯＮＥＴの仕様に従って制御コマンドの変更などを行い、エアコン２７５７に対して制御コマンドを発行する。

【０２２４】図５０に示すフローチャートを参照して、制限項目作成部１３１の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部１２３に図４６に示す情報が格納されており、初期制限項目格納部１３２に図４９に示す初期制限項目が格納されており、図４８に示す個別制限項目において、宅外ネットワークであるインターネット１６０に接続されている制御端末１４１に係る制限項目（図中の新項目Ａ）が未登録である状況を想定して説明する。ただし、図５０において、図２５に示すフローと同一の処理ステップについては同一の参照符号を付す。

【０２２５】制限項目作成部１３１は、ステップＳ９０１で、制御コマンド判定部２７１２より、制限項目を作成する際の条件として、機器識別子と、制御端末のネットワーク情報と、機器カテゴリーとを受け取る。ここで受け取る項目は以下の通りである。

【０２２６】機器識別子＝０ｘ０００３
制御端末のネットワーク情報＝宅外
機器カテゴリー＝空調機器

【０２２７】ステップＳ９０２で、機器識別子と制御端末のネットワーク情報とをもとに、個別制限項目格納部１３３に対し個別制限項目を送るよう要求する。ステップＳ９０３で、ステップＳ９０２の要求に対する条件に一致する制限項目を受け取る。ただし、ここでの説明の例では、条件に対応した制限項目がなかったことが通知される。ステップＳ９０４で、制限情報がない条件が存在するか否かを確認する。制限情報がない条件が存在すれば、以下のステップＳ９０５に進み、存在しなければ、ステップＳ９０８に進む。ここでの説明の例では、

ステップＳ９０５に進む。

【０２２８】ステップＳ９０５で、制限情報が存在しない条件について、初期制限項目格納部１３２に対して、この条件に対応する制限項目を通知するように要求する。ステップＳ９０６で、ステップＳ９０５の要求に対する条件に一致する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【０２２９】制御端末のネットワーク情報＝宅外
機器カテゴリー＝空調機器
制限情報＝アクセス許可

【０２３０】ステップＳ９０７で、ステップＳ９０６で受け取った制限項目を個別制限項目格納部１３３に登録する。この結果、図４８に新項目Ａで示した個別制限項目が新たに登録される。ステップＳ９０８で、条件と制限情報とを対応づけて、制御コマンド判定部２７１２に通知する。この結果、宅外ネットワークからエアコン２７５７を制御することは、制限情報＝アクセス許可であるため、制御コマンド判定部２７１２は、制御端末１４１に対して、実行許可の通知を行う。なお、このとき、通知された制限情報がアクセス不可であった場合には、制御コマンド判定部２７１２は、制御コマンド送受信部２７１３を通じて制御端末１４１に対し制御不可の通知を行い、制御端末１４１は、その通知を受けて、例えば「この制御コマンドに対する権限を有しておりません」等の画面表示を行う。

【０２３１】なお、個別制限項目格納部１３３に格納されている個別制限項目は、入力部１３４よりユーザが設定することができる。これは、制限項目作成部１３１で作成されて登録された制限項目についても同様である。また、初期制限項目格納部１３２に格納されている初期制限項目についても、入力部１３４よりユーザが設定することができる。

【０２３２】なお、本実施形態では、宅外からのアクセスとして、インターネット１６０に接続されている制御端末１４１より制御コマンドの発行を行ったが、宅外ネットワークはインターネット以外でもよく、また、宅内のＩＰネットワーク２７８０やＩＥＥＥ１３９４バス１７０やＥＣＨＯＮＥＴ２７９０またはその他のネットワークに接続されている制御端末より制御コマンドの発行を行って、被制御端末を制御しても構わない。例えば、宅内からのアクセスとして、ＰＣ２７５５より制御コマンドを発行して被制御装置を制御しても構わない。

【０２３３】また、本実施形態では、宅内のネットワークとしてＩＥＥＥ１３９４バス１７０、ＩＰネットワーク２７８０、ＥＣＨＯＮＥＴ２７９０を取り上げ、宅外のネットワークとしてインターネット１６０を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、Ｂｌｕｅｔｏｏｔｈなどが挙げられる。

【０２３４】また、本実施形態では、４つのネットワークが通信装置２７００に接続される例を示したが、これに限らず、通信装置２７００に接続されるネットワークの数は１から３または５以上であっても構わない。

【０２３５】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、２つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

【０２３６】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリーや、サービス情報や、ユーザＩＤや、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【０２３７】また、本実施形態では、被制御端末として、ＰＣ、ビデオ、およびエアコンを例に挙げたが、ＰＣが通信装置を通じてビデオを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【０２３８】また、本実施形態では、機器カテゴリーの分類項目としてＡＶ機器や空調機器などを使用したが、ビデオやチューナなど他の分類を行っても構わない。

【０２３９】また、本実施形態では、ネットワーク情報格納部１２３に格納されている要素情報に基づいて予めメニューを作成しておくとしたが、それに代えて、制御コマンド送受信部２７１３からメニューを要求された時点で、ネットワーク情報取得部１２２が要素情報を取得してメニューを作成するようにしても構わない。予めメニューを作成しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、メニューを必要に応じて作成する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【０２４０】また、本実施形態では、制御端末１４１から制御コマンドを発行した際に新たなサービスに係る制限項目の作成を行ったが、新たなサービスを検出した段階でこれを行っても構わない。この場合、前者と比較し、ユーザが制御コマンドを発行してから、制御コマンド中継部２７１０がこの制御コマンドの有効性を判断して被制御端末に向けて発行するまでの時間が短くなるため好ましい。

【０２４１】以上のように、第５の実施形態によれば、対応する個別制限項目が存在しない場合、初期制限項目を用いてアクセス制限を行うため、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【０２４２】また、通信装置がユーザに対して送信する制御メニューにアクセス制限の内容を反映させる前述の第２の実施形態等と比較し、制御端末が発行した制御コ

マンドに対してアクセス制限を行うことができる。

【０２４３】また、制御端末および被制御端末のネットワークによってアクセス制限を設定しているため、例えば宅外ネットワークとしてインターネットのように不特定多数が利用するネットワークに対してはアクセス不可とし、ＩＥＥＥ１３９４バスのような宅内のネットワークであればアクセス許可するというように、利便性と安全性を両立した制御が可能となる。

【０２４４】次に、本件発明の実施形態から把握できる請求項以外の技術思想を、その効果とともに記載する。

【０２４５】第１の発明は、単一または複数のネットワークに接続され、このネットワークに接続される複数の機器のうちのある機器による他の機器に対する制御を条件に応じて制限する通信装置であって、ネットワークおよびネットワークに接続される機器に関する情報を要素情報として取得するディレクトリ管理手段と、要素情報と、他の機器を制御する機器である制御端末に関する情報と、この制御端末を使用して制御を行おうとするユーザの識別子との少なくともいずれかを含む情報を制御条件として、この制御条件に合致する場合の制御の可否を規定する制限情報とともに個別制限項目として管理する制限項目管理手段と、要素情報および個別制限項目に基づいて、機器間の制御を制限する制御制限手段とを備え、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、この制御条件に応じてこの制御条件に係る個別制限項目を動的に新たに作成することを特徴とする。

【０２４６】上記のように、第１の発明によれば、ネットワーク上に新たな機器が接続されたときなど、ネットワーク上の機器間で制御を行う際に、その制御の可否を示す情報が登録されていない場合であっても、この制御の可否を示す制限項目を動的に作成するため、ユーザがその都度設定を行う必要がなく、ネットワークに対して十分な知識がないユーザがネットワーク機器を接続した場合でも、ネットワークのセキュリティを確保したまま、ネットワークを通じて制御することが可能となる。またこのとき、ネットワークに接続される機器に関する情報や、制御端末に関する情報、例えば、制御端末が所属するネットワークに関する情報や表示能力・再生能力等の制御端末の性能に関する情報や、制御を行おうとするユーザの識別子の情報やその他種々の条件またはその組合せに応じて、動的に好ましい設定を行うことができる。

【０２４７】第２の発明は、第１の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納手段を含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２４８】上記のように、第２の発明によれば、個別制限項目に存在しない制御条件に対して制限を行うために、予め設定された初期制限項目から制御条件に合致した好ましい制限項目を作成するので、例えば新たな機器がネットワークに接続された際でも、その機器に対して予め設定された初期制限項目に基づいて好ましい設定を自動的に設定することができる。

【０２４９】第３の発明は、第１の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、この選出された個別制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２５０】上記のように、第３の発明によれば、制御条件に合致した個別制限項目が登録されていない場合であっても、すでに登録されている個別制限項目の中から、この制御条件が一部の条件を除いて一致するものをもとに、この制御条件に対する制御の可否を自動的に設定することができる。なお、一部の条件としては、例えば、機器識別子や、制御端末を操作するユーザの識別子などであり、これにより、例えば、ネットワークに新たな機器が接続され、この機器の識別子に対する制限項目がまだ登録されていない場合であっても、すでに登録されている個別制限項目の中からこの機器の識別子を除いて条件が一致するものを参照して類推することにより、予め特別な設定を必要とすることなく、好ましい設定を自動的に行うことができる。

【０２５１】第４の発明は、第３の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、選出した個別制限項目に含まれる制限情報の全てにおいて制御許可が規定されている場合には、この制御条件に係る個別制限項目として、制御許可を規定する制限情報を含む個別制限項目を新たに作成し、一方、選出した個別制限項目に含まれる制限情報のいずれかにおいて制御不許可が規定されている場合には、この制御条件に係る個別制限項目として、制御不許可を規定する制限情報を含む個別制限項目を新たに作成することを特徴とする。

【０２５２】上記のように、第４の発明によれば、制御を制限しようとする制御条件に対して、選出した個別制限項目において全て制御許可である場合のみ、制御許可として制限情報を設定するため、自動的に制限項目を設定することによって、本来制御が許可されるべきでない条件に対して、勝手に制御許可として登録してしまう危

険を回避し、より安全に制限項目の自動設定が行える。

【０２５３】第５の技術思想は、第１の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納手段を含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在する場合には、この制御条件に関連する個別制限項目に含まれる制限情報に基づいて、この制御条件に係る個別制限項目を新たに作成し、一方、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在しない場合には、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２５４】上記のように、第５の発明によれば、制限項目がまだ登録されていない制御条件に対して、この制御条件に対する制限情報を類推するための個別制限項目が、一定数以上存在する場合にはそれら個別制限項目から類推して制限情報を設定し、一方、一定数以上存在しない場合には、初期制限項目に基づいて設定する。よって、制御条件に対して制限情報を類推するための材料となる個別制限項目が少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

【０２５５】第６の発明は、第１の発明において、制御制限手段は、制限項目管理手段によって管理される個別制限項目に基づいて、制御端末が制御可能であるサービスについてのみからなる制御メニューをこの制御端末に送信することにより、制御端末による制御を制限することを特徴とする。

【０２５６】上記のように、第６の発明によれば、制御端末に通知する制御メニュー自体の内容に制限内容を反映させることにより、機器の制御を容易に制限することができる。また、制御を行おうとするユーザは、事前に制御可能な内容を知ることができるため、制御コマンドを実行するまで制御の可否が分からないという問題もなく機器の制御を行うことができる。

【０２５７】第７の発明は、第１の発明において、制御制限手段は、制限項目管理手段によって管理される個別制限項目に基づいて、制御端末が発行した制御コマンドのうち、この制御端末が制御可能であるサービスに係る制御コマンドのみを制御対象の機器に送信することにより、制御端末による制御を制限することを特徴とする。

【０２５８】上記のように、第７の発明によれば、ユーザが制御端末からコマンドが発生された時点で制御の可否を判断するため、例えば制限項目が変更された直後であっても、その変更内容が即座に制御の制限に反映されることになり、より確実な制限が容易に可能となる。

【０２５９】第８の発明は、第１の発明において、ディレクトリ管理手段は、ネットワークに新たな機器が接続されたことを検出する構成要素検出手段を含む。

【０２６０】上記のように、第８の発明によれば、ネットワークに新たな機器が接続されたときに、これを検出することができるため、ディレクトリ管理手段において最新の要素情報を自動的に取得することができる。

【０２６１】第９の発明は、第１の発明において、制御条件は、制御端末の属するネットワークが宅内のネットワークであるか宅外のネットワークであるかに関する条件を含む。

【０２６２】上記のように、第９の発明によれば、宅内からのアクセスか宅外からのアクセスかに応じて制御を制限することができるため、例えば、宅内からのアクセスは許可して、宅外からのアクセスは不可にするなど、安全性の高い設定を動的に設定することができる。

【０２６３】第１０の発明は、単一または複数のネットワークに接続される複数の機器のうちのある機器による他の機器に対する制御を条件に応じて制限する通信制限方法であって、ネットワークおよびネットワークに接続される機器に関する情報を要素情報として取得するディレクトリ管理ステップと、要素情報と、他の機器を制御する機器である制御端末に関する情報と、この制御端末を使用して制御を行おうとするユーザの識別子との少なくともいずれかを含む情報を制御条件として、この制御条件に合致する場合の制御の可否を規定する制限情報とともに個別制限項目として管理する制限項目管理ステップと、要素情報および個別制限項目に基づいて、機器間の制御を制限する制御制限ステップとを備え、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、この制御条件に応じてこの制御条件に係る個別制限項目を動的に新たに作成することを特徴とする。

【０２６４】上記のように、第１０の発明によれば、ネットワーク上に新たな機器が接続されたときなど、ネットワーク上の機器間で制御を行う際に、その制御の可否を示す情報が登録されていない場合であっても、この制御の可否を示す制限項目を動的に作成するため、ユーザがその都度設定を行う必要がなく、ネットワークに対して十分な知識がないユーザがネットワーク機器を接続した場合でも、ネットワークのセキュリティを確保したまま、ネットワークを通じて制御することが可能となる。またこのとき、ネットワークに接続される機器に関する情報や、制御端末に関する情報、例えば、制御端末が所属するネットワークに関する情報や表示能力・再生能力等の制御端末の性能に関する情報や、制御を行おうとするユーザの識別子の情報やその他種々の条件またはその組合せに応じて、動的に好ましい設定を行うことができる。

【０２６５】第１１の発明は、第１０の発明において、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納ステップを含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２６６】上記のように、第１１の発明によれば、個別制限項目に存在しない制御条件に対して制限を行うために、予め設定された初期制限項目から制御条件に合致した好ましい制限項目を作成するので、例えば新たな機器がネットワークに接続された際でも、その機器に対して予め設定された初期制限項目に基づいて好ましい設定を自動的に設定することができる。

【０２６７】第１２の発明は、第１０の発明において、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、この選出された個別制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２６８】上記のように、第１２の発明によれば、制御条件に合致した個別制限項目が登録されていない場合であっても、すでに登録されている個別制限項目の中から、この制御条件が一部の条件を除いて一致するものをもとに、この制御条件に対する制御の可否を自動的に設定することができる。なお、一部の条件としては、例えば、機器識別子や、制御端末を操作するユーザの識別子などであり、これにより、例えば、ネットワークに新たな機器が接続され、この機器の識別子に対する制限項目がまだ登録されていない場合であっても、すでに登録されている個別制限項目の中からこの機器の識別子を除いて条件が一致するものを参照して類推することにより、予め特別な設定を必要とすることなく、好ましい設定を自動的に行うことができる。

【０２６９】第１３の発明は、第１２の発明において、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、選出した個別制限項目に含まれる制限情報の全てにおいて制御許可が規定されている場合には、この制御条件に係る個別制限項目として、制御許可を規定する制限情報を含む個別制限項目を新たに作成し、一方、選出した個別制限項目に含まれる制限情報のいずれかにおいて制御不許可が規定されている場合には、この制御条件に係る個別制限項目として、制御不許可を規定する制限情報を含む個別制限項目を新たに作成することを特徴とする。

【０２７０】上記のように、第１３の発明によれば、制御を制限しようとする制御条件に対して、選出した個別制限項目において全て制御許可である場合のみ、制御許可として制限情報を設定するため、自動的に制限項目を設定することによって、本来制御が許可されるべきでない条件に対して、勝手に制御許可として登録してしまう危険を回避し、より安全に制限項目の自動設定が行える。

【０２７１】第１４の発明は、第１０の発明において、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納ステップを含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在する場合には、この制御条件に関連する個別制限項目に含まれる制限情報に基づいて、この制御条件に係る個別制限項目を新たに作成し、一方、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在しない場合には、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【０２７２】上記のように、第１４の発明によれば、制限項目がまだ登録されていない制御条件に対して、この制御条件に対する制限情報を類推するための個別制限項目が、一定数以上存在する場合にはそれら個別制限項目から類推して制限情報を設定し、一方、一定数以上存在しない場合には、初期制限項目に基づいて設定する。よって、制御条件に対して制限情報を類推するための材料となる個別制限項目が少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

【０２７３】第１５の発明は、第１０の発明において、制御制限ステップは、制限項目管理ステップによって管理される個別制限項目に基づいて、制御端末が制御可能であるサービスについてのみからなる制御メニューをこの制御端末に送信することにより、制御端末による制御を制限することを特徴とする。

【０２７４】上記のように、第１５の発明によれば、制御端末に通知する制御メニュー自体の内容に制限内容を反映させることにより、機器の制御を容易に制限することができる。また、制御を行おうとするユーザは、事前に制御可能な内容を知ることができるため、制御コマンドを実行するまで制御の可否が分からないという問題もなく機器の制御を行うことができる。

【０２７５】第１６の発明は、第１０の発明において、制御制限ステップは、制限項目管理ステップによって管

理される個別制限項目に基づいて、制御端末が発行した制御コマンドのうち、この制御端末が制御可能であるサービスに係る制御コマンドのみを制御対象の機器に送信することにより、制御端末による制御を制限することを特徴とする。

【０２７６】上記のように、第１６の発明によれば、ユーザが制御端末からコマンドが発生された時点で制御の可否を判断するため、例えば制限項目が変更された直後であっても、その変更内容が即座に制御の制限に反映されることになり、より確実な制限が容易に可能となる。

【０２７７】第１７の発明は、第１０の発明において、ディレクトリ管理ステップは、ネットワークに新たな機器が接続されたことを検出する構成要素検出ステップを含む。

【０２７８】上記のように、第１７の発明によれば、ネットワークに新たな機器が接続されたときに、これを検出することができるため、ディレクトリ管理手段において最新の要素情報を自動的に取得することができる。

【０２７９】第１８の発明は、第１０の発明において、制御条件は、制御端末の属するネットワークが宅内のネットワークであるか宅外のネットワークであるかに関する条件を含む。

【０２８０】上記のように、第１８の発明によれば、宅内からのアクセスか宅外からのアクセスかに応じて制御を制限することができるため、例えば、宅内からのアクセスは許可して、宅外からのアクセスは不可にするなど、安全性の高い設定を動的に設定することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るファイアウォール装置の基本的構成を示す図である。

【図２】本発明の第１の実施形態に係るファイアウォール装置の内部ハードウエア基本構成を示すブロック図である。

【図３】本発明の第１の実施形態に係るファイアウォール装置のソフトウエア基本構成を示すブロック図である。

【図４】本発明の第１の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作を示すフローチャートである。

【図５】図４のステップＳ１０４のサブルーチンを示すフローチャートである。

【図６】本発明の第１の実施形態に係るファイアウォール装置の認証サービスに対して、通信路が外部から設定される動作を示すフローチャートである。

【図７】本発明の第１の実施形態に係るファイアウォール装置が行うサービス有効期限管理の動作を示すフローチャートである。

【図８】本発明の第１の実施形態に係るファイアウォール装置のディレクトリ管理機能部に格納されているサービス情報の一例を示す図である。

【図９】本発明の第１の実施形態に係るファイアウォール装置のディレクトリ管理機能部に予め設定されているサービス基本公開ポリシーの一例を示す図である。

【図１０】本発明の第１の実施形態に係るファイアウォール装置のディレクトリ管理機能部に設定されるサービス詳細公開ポリシーの一例を示す図である。

【図１１】本発明の第１の実施形態に係るファイアウォール装置の内部ネットワークから外部ネットワークへの通信を許可するためのＩＰフィルタ機能部に設定されるパケットフィルタの情報を示す図である。

【図１２】本発明の第１の実施形態に係るファイアウォール装置のＦＴＰサービスの通信シーケンスと、ディレクトリ管理機能部３３によってアドレス変換機能部２５に設定されるアドレス変換テーブルと、ＩＰフィルタ機能部２３に設定されるパケットフィルタとを示す図である。

【図１３】本発明の第１の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作の一部を示すフローチャートである。

【図１４】本発明の第１の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作の一部を示すフローチャートである。

【図１５】本発明の第１の実施形態に係るファイアウォール装置のディレクトリ管理機能部に格納されているサービス情報の一例を示す図である。

【図１６】本発明の第１の実施形態に係るファイアウォール装置のディレクトリ管理機能部に設定されるサービス詳細公開ポリシーの一例を示す図である。

【図１７】本発明の第２の実施形態に係る通信装置１００およびそれに接続されるネットワークおよび機器の構成を示す図である。

【図１８】通信装置１００のネットワーク情報格納部１２３に格納される情報の一例を示す図である。

【図１９】ＩＥＥＥ１３９４バス１７０に新たに被制御端末１５１が接続されたときの通信装置１００の動作を示すシーケンス図である。

【図２０】制御端末１４１において通信装置１００から取得した制御メニューの表示の一例を示す図である。

【図２１】通信装置１００の個別制限項目格納部１３３に格納される個別制限項目の一例を示す図である。

【図２２】通信装置１００の個別制限項目格納部１３３に格納される個別制限項目の他の一例を示す図である。

【図２３】制御端末１４１から制御メニューの要求を受けたときの通信装置１００の動作を示すシーケンス図である。

【図２４】通信装置１００の初期制限項目格納部１３２に格納される初期制限項目の一例を示す図である。

【図２５】通信装置１００の制限項目作成部１３１の動作を示すフローチャートである。

【図２６】制御端末１４１において通信装置１００から

取得した制御メニューの表示の一例を示す図である。
【図２７】本発明の第３の実施形態に係る通信装置１０００およびそれに接続されるネットワークおよび機器の構成を示す図である。
【図２８】ＩＥＥＥ１３９４バス１７０に新たに被制御端末１５１が接続されたときの通信装置１０００の動作を示すシーケンス図である。
【図２９】通信装置１０００のネットワーク情報格納部１２３に格納される情報の一例を示す図である。
【図３０】制御端末１４１から制御メニューの要求を受けたときの通信装置１０００の動作を示すシーケンス図である。
【図３１】通信装置１０００の個別制限項目格納部１３３に格納される個別制限項目の一例を示す図である。
【図３２】通信装置１０００の制限項目作成部１３１の動作を示すフローチャートである。
【図３３】制御端末１４１において通信装置１０００から取得した制御メニューの表示の一例を示す図である。
【図３４】制御端末１４１において通信装置１０００から取得した制御メニューの表示の一例を示す図である。
【図３５】本発明の第４の実施形態に係る通信装置１８００およびそれに接続されるネットワークおよび機器の構成を示す図である。
【図３６】ＩＥＥＥ１３９４バス１７０に新たに被制御端末１５１が接続されたときの通信装置１８００の動作を示すシーケンス図である。
【図３７】通信装置１８００のネットワーク情報格納部１２３に格納される情報の一例を示す図である。
【図３８】制御端末１４１から制御メニューの要求を受けたときの、特に、条件に合致する制限項目の数が３未満である場合の通信装置１８００の動作を示すシーケンス図である。
【図３９】通信装置１８００の個別制限項目格納部１３３に格納される個別制限項目の一例を示す図である。
【図４０】通信装置１８００の初期制限項目格納部１３２に格納される初期制限項目の一例を示す図である。
【図４１】制御端末１４１から制御メニューの要求を受けたときの、特に、条件に合致する制限項目の数が３以上である場合の通信装置１８００の動作を示すシーケンス図である。
【図４２】通信装置１８００の制限項目作成部１８３１の動作を示すフローチャートである。
【図４３】制御端末１４１において通信装置１８００から取得した制御メニューの表示の一例を示す図である。
【図４４】本発明の第５の実施形態に係る通信装置２７００およびそれに接続されるネットワークおよび機器の構成を示す図である。
【図４５】サービス情報を取得するときの通信装置２７００の動作を示すシーケンス図である。
【図４６】通信装置２７００のネットワーク情報格納部１２３に格納される情報の一例を示す図である。
【図４７】制御端末１４１から制御メニューの要求を受けたときの通信装置２７００の動作を示すシーケンス図である。
【図４８】通信装置２７００の個別制限項目格納部１３３に格納される個別制限項目の一例を示す図である。
【図４９】通信装置２７００の初期制限項目格納部１３２に格納される初期制限項目の一例を示す図である。
【図５０】通信装置２７００の制限項目作成部１３１の動作を示すフローチャートである。
【図５１】従来のネットワークサービス管理方式におけるネットワークの全体構成を示す図である。
【図５２】従来のネットワークサービス管理方式においてネットワーク管理者に提供されるネットワーク情報を示す図である。
【図５３】従来のネットワークサービス管理方式においてサービス管理者に提供されるネットワーク情報を示す図である。
【図５４】従来のネットワークサービス管理方式においてユーザ端末を使用するユーザに提供されるネットワーク情報を示す図である。
【符号の説明】
１…ＨＧＷ
２…サーバ
３…外部端末
１０…ＣＰＵ
１１、２２…メモリ
２０…スイッチ部
２１…コントローラ
２３…ＩＰフィルタ機能部
２４…フォワーディング機能部
２５…アドレス変換部
２６…ＰＨＹ・ＭＡＣ機能部
３１…通信部
３２…認証機能部
３３…ディレクトリ管理機能部
３４…通信路設定機能部
１００…通信装置
１１０…制御メニュー構成部
１１１…制御メニュー作成要求受信部
１１２…制御メニュー作成部
１１３…制御メニュー送信部
１２０…ディレクトリ管理機能部
１２１…ネットワーク構成要素検出部
１２２…ネットワーク情報取得部
１２３…ネットワーク情報格納部
１３０…制限項目管理部
１３１…制限項目作成部
１３２…初期制限項目格納部
１３３…個別制限項目格納部

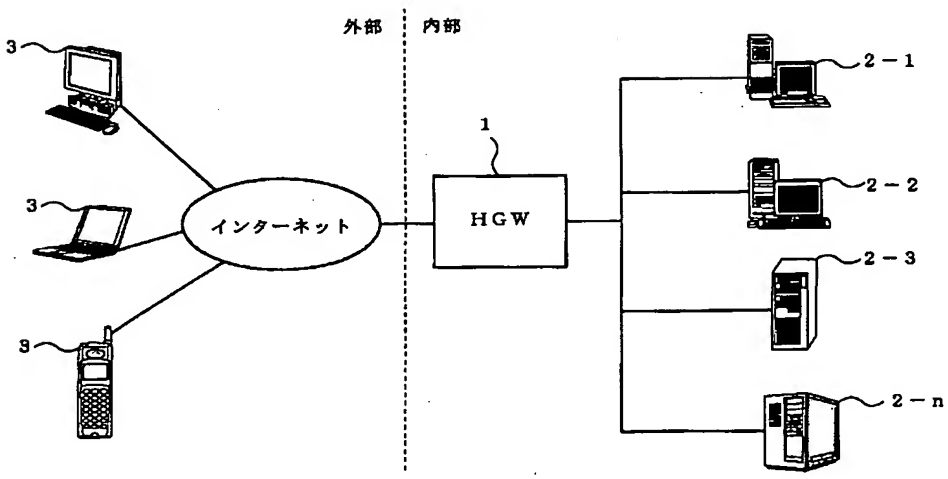
69

１３４…入力部
１４１…制御端末
１５１、１５２、１５３…被制御端末
１６０…インターネット
１７０…ＩＥＥＥ１３９４バス
１０００…通信装置
１０３０…制限項目管理部
１０３１…制限項目作成部
１０５４…被制御端末
１８００…通信装置
１８３０…制限項目管理部

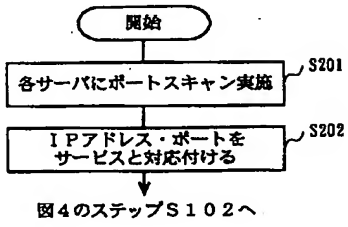
70

１８３１…制限項目作成部
２７００…通信装置
２７１０…制御コマンド中継部
２７１２…制御コマンド判定部
２７１３…制御コマンド送受信部
２７２０…ディレクトリ管理機能部
２７２４…ＩＥＥＥ１３９４プロトコル変換部
２７２５…ＥＣＨＯＮＥＴプロトコル変換部
２７８０…インターネット
２７９０…ＥＣＨＯＮＥＴ
２７５５、２７５６、２７５７…被制御端末

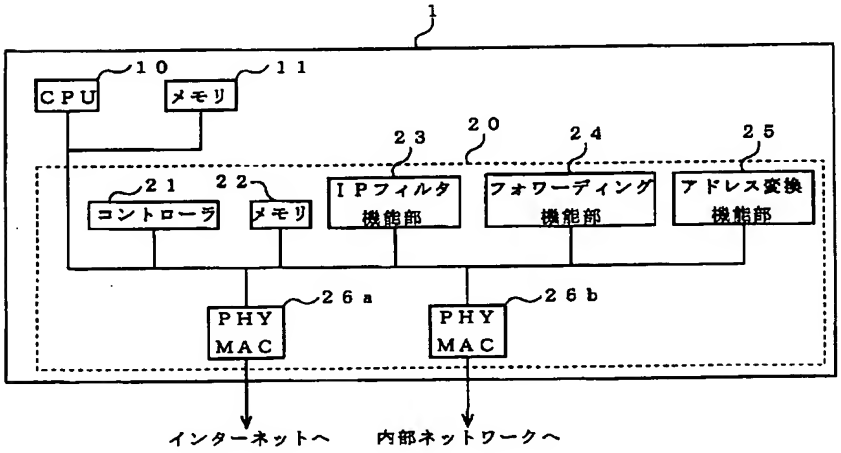
【図１】



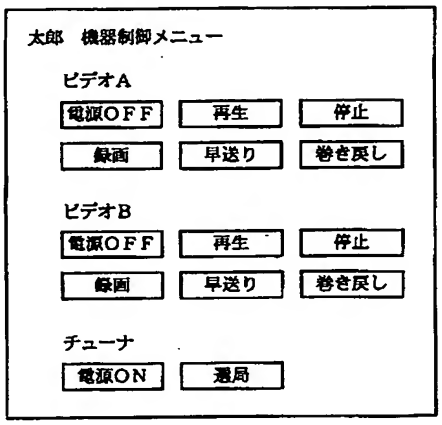
【図１３】



【図２】



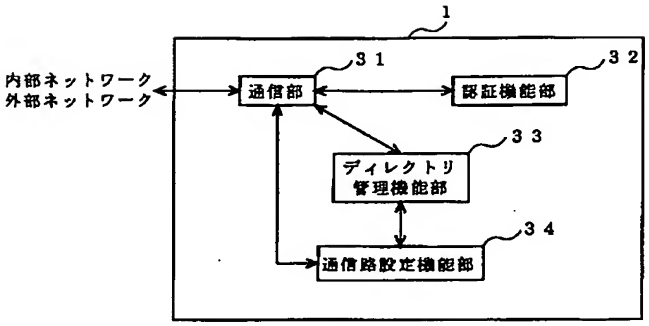
【図２０】



【図１１】

方向	SA	DA	プロトコル	SP	DP	ACK	
外	LA	IA	TCP	LP	IP	－	デフォルト設定A
内	IA	LA	TCP	IP	LP	YES	デフォルト設定B

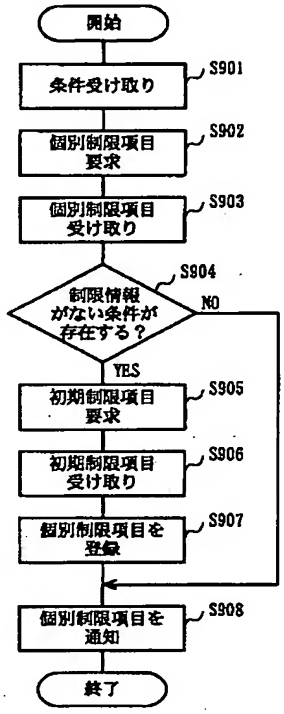
【図３】



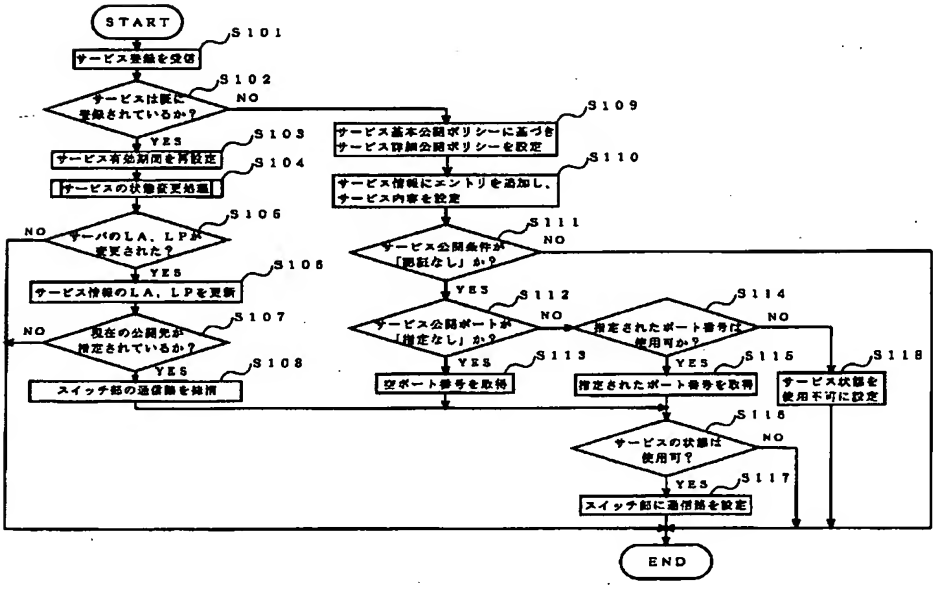
【図９】

サービス種別	公開先相手	公開条件	公開ポート
SMTPサーバ	全て公開	認証なし	25
FTPサーバ	TAROU、HANAKO	認証後公開	21
HTTPサーバ	TAROU	認証後公開	指定なし
TELNET	非公開	－	－
NNTPサーバ	１９２．１６８．５１．５０	認証なし	119

【図２５】



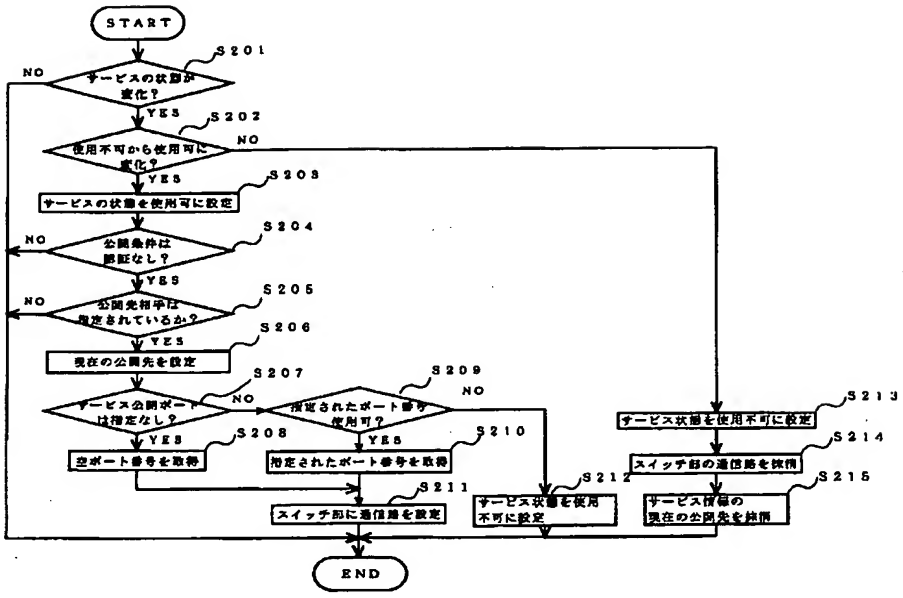
【図４】



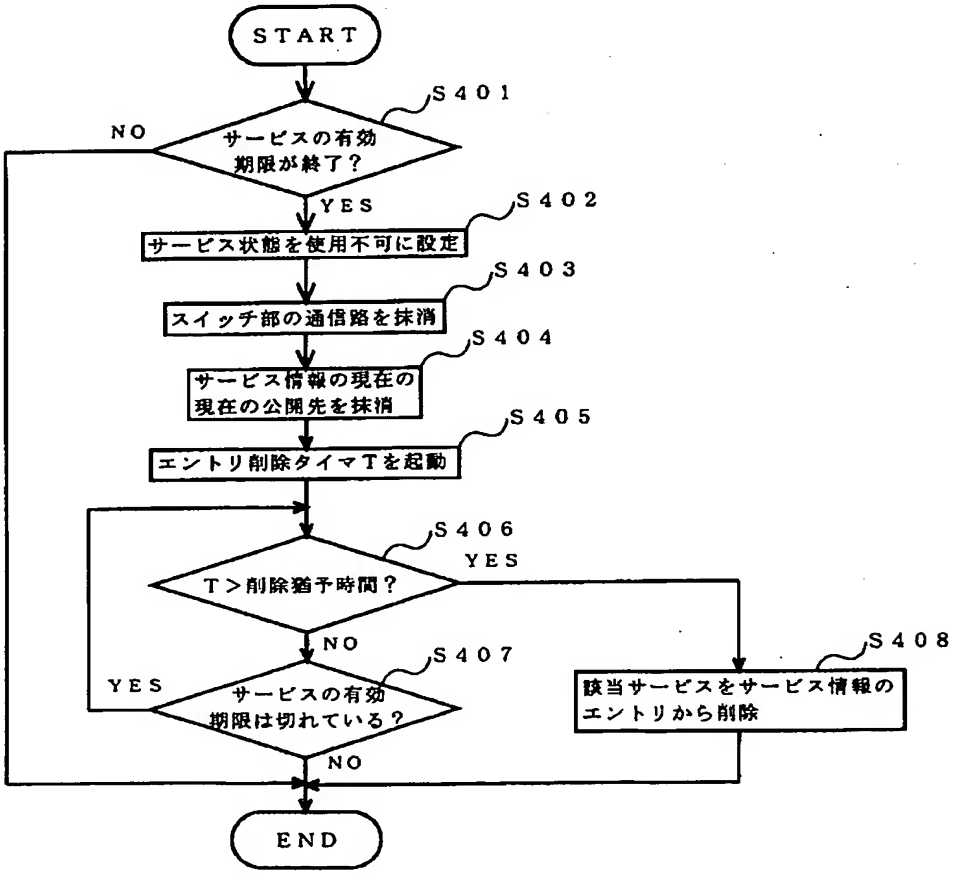
【図８】

サービス名	サービス アドレス	プロトコル	外部公開 ポート番号	現在の公開先	サービス 有効期間	状態
SMTP	PC001 IP：LA2 PORT：25	TCP／IP	25	全て	0:31:21	使用可
FTP	PC001 IP：LA2 PORT：21	TCP／IP	－	－	0:31:21	使用可
HTTP	PC001 IP：LA2 PORT：8080	TCP／IP	2048	TAROU IP：IA1 PORT：1025	0:31:21	使用可
FTP	PC002 IP：LA3 PORT：21	TCP／IP	21	HANAKO IP：IA3 PORT：1024	0:55:35	使用可

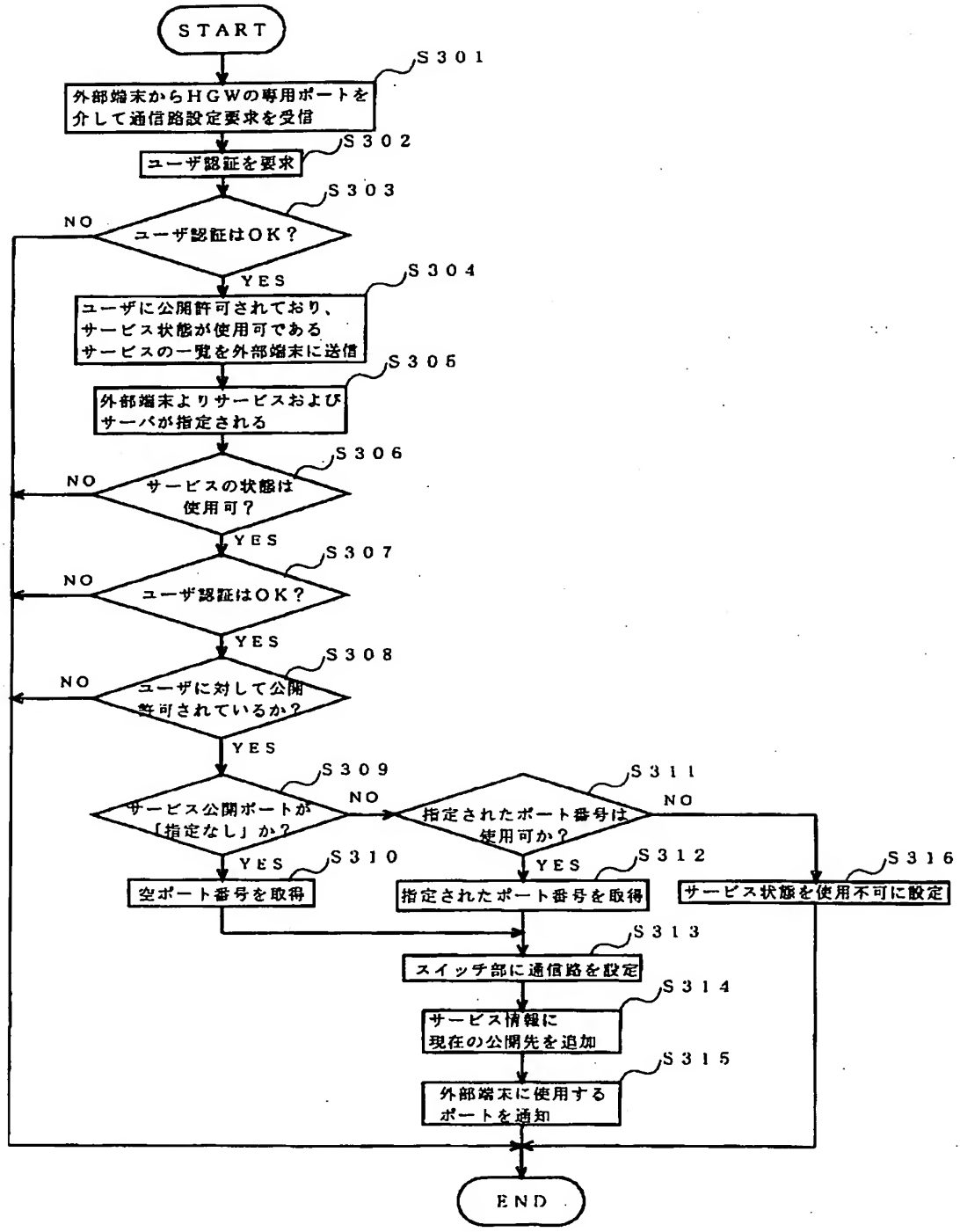
【図５】


START
S201
サービスの状態が変化？
NO
YES
S202
使用不可から使用可に変化？
NO
YES
S203
サービスの状態を使用可に設定
S204
公開条件は認証なし？
NO
YES
S205
公開先相手は指定されているか？
NO
YES
S206
現在の公開先を設定
S207
サービス公開ポートは指定なし？
NO
YES
S208
空ポート番号を取得
S209
指定されたポート番号使用可？
NO
YES
S210
指定されたポート番号を取得
S211
スイッチ部に通信路を設定
S212
サービス状態を使用不可に設定
S213
サービス状態を使用不可に設定
S214
スイッチ部の通信路を抹消
S215
サービス情報の現在の公開先を抹消
END

【図７】


START
S401
サービスの有効期限が終了？
NO
YES
S402
サービス状態を使用不可に設定
S403
スイッチ部の通信路を抹消
S404
サービス情報の現在の現在の公開先を抹消
S405
エントリ削除タイマＴを起動
S406
Ｔ＞削除猶予時間？
YES
NO
S407
サービスの有効期限は切れている？
YES
NO
S408
該当サービスをサービス情報のエントリから削除
END

【図６】



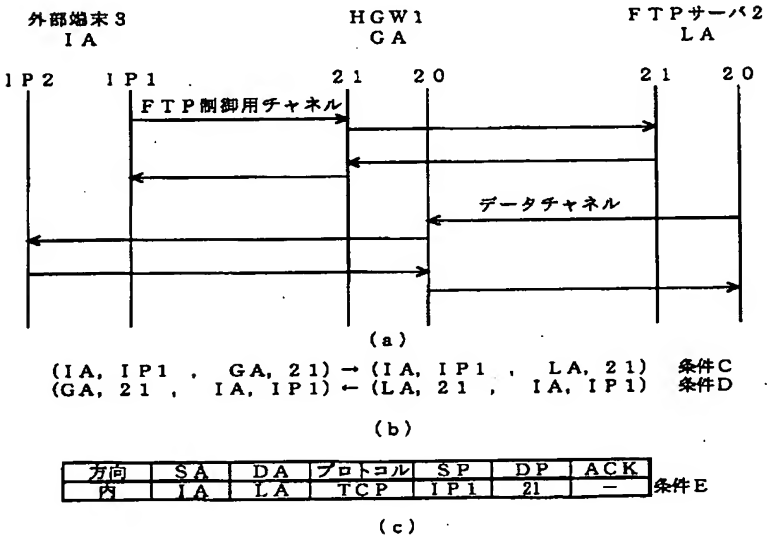
【図１８】

GUID	機器カテゴリー	サービス情報	所属ネットワーク
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止	ＩＥＥＥ１３９４
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止	ＩＥＥＥ１３９４
0x0123456789034567	チューナ	電源、選局	ＩＥＥＥ１３９４

【図１０】

サーバ名	サービス種別	公開先相手	公開条件	公開ポート
サーバ２－１	SMTPサーバ	全て公開	認証なし	25
	FTPサーバ	TAROU、HANAKO	認証後公開	21
	HTTPサーバ	TAROU	認証後公開	指定なし
	TELNET	非公開	－	－
サーバ２－２	FTPサーバ	HANAKO	認証後公開	21
	HTTPサーバ	HANAKO	認証後公開	指定なし
	TELNET	HANAKO	認証後公開	指定なし

【図１２】



（ａ）

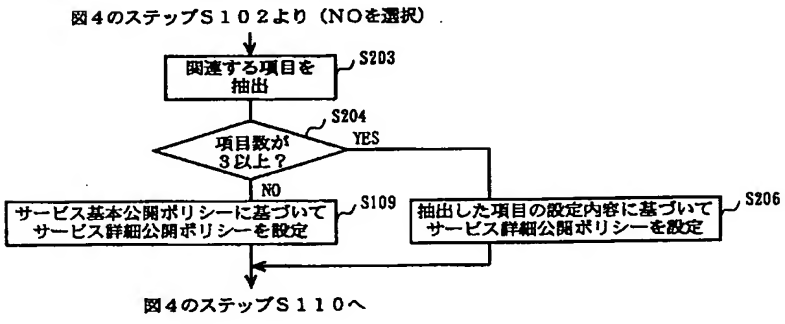
（ＩＡ，ＩＰ１，ＧＡ，２１）→（ＩＡ，ＩＰ１，ＬＡ，２１）　条件Ｃ
（ＧＡ，２１，ＩＡ，ＩＰ１）←（ＬＡ，２１，ＩＡ，ＩＰ１）　条件Ｄ

（ｂ）

方向	ＳＡ	ＤＡ	プロトコル	ＳＰ	ＤＰ	ＡＣＫ	
内	ＩＡ	ＬＡ	ＴＣＰ	ＩＰ１	21	－	条件Ｅ

（ｃ）

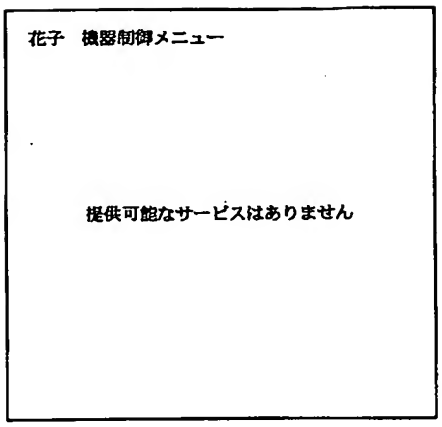
【図１４】



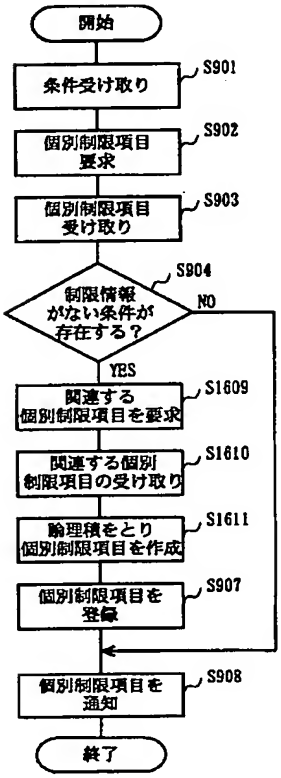
【図２９】

ＧＵＩＤ	機器カテゴリー	サービス情報
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123466789034567	ビデオ	電源、録画、再生、早送り、巻き戻し、停止

【図２６】



【図３２】



【図１５】

サービス名	サービス アドレス	プロトコル	外部公開 ポート番号	現在の公開先	サービス 有効期間	状態
SMTP	PC001 IP:LA2 PORT:25	TCP／IP			0:31:21	使用可
FTP	PC001 IP:LA2 PORT:21	TCP／IP			0:31:21	使用可
HTTP	PC001 IP:LA2 PORT:8080	TCP／IP			0:31:21	使用可
FTP	PC002 IP:LA3 PORT:21	TCP／IP			0:55:35	使用可
FTP	PC003 IP:LA4 PORT:21	TCP／IP			0:59:55	使用可
HTTP	PC004 IP:LA5 PORT:8080	TCP／IP			0:59:55	使用可
FTP	PC004 IP:LA5 PORT:21	TCP／IP			0:59:55	使用可

新たに追加される サービス情報

【図１６】

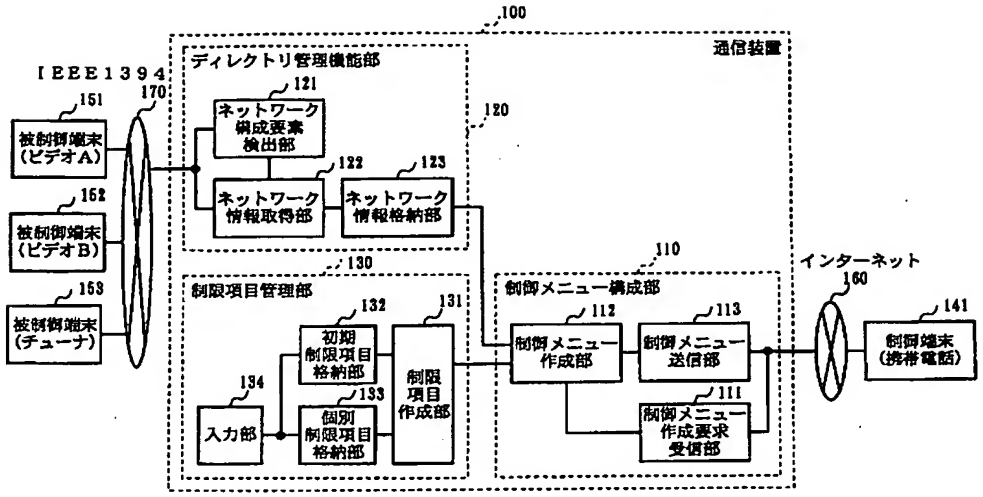
	サーバ名	サービス種別	公開先相手	公開条件	公開ポート
	サーバ２－１	SMTPサーバ	全て公開	認証なし	25
項目C→		FTPサーバ	TAROU, HANAKO	認証後公開	21
項目A→		HTTPサーバ	TAROU	認証後公開	指定なし
		TELNET	非公開	－	－
項目D→	サーバ２－２	FTPサーバ	TAROU, HANAKO	認証後公開	21
項目B→		HTTPサーバ	HANAKO	認証後公開	指定なし
		TELNET	HANAKO	認証後公開	指定なし
項目E→	サーバ２－３	FTPサーバ	TAROU, HANAKO	認証後公開	21
	サーバ２－４	HTTPサーバ	TAROU	認証後公開	指定なし
		FTPサーバ	TAROU, HANAKO	認証後公開	21

新たに追加される 項目

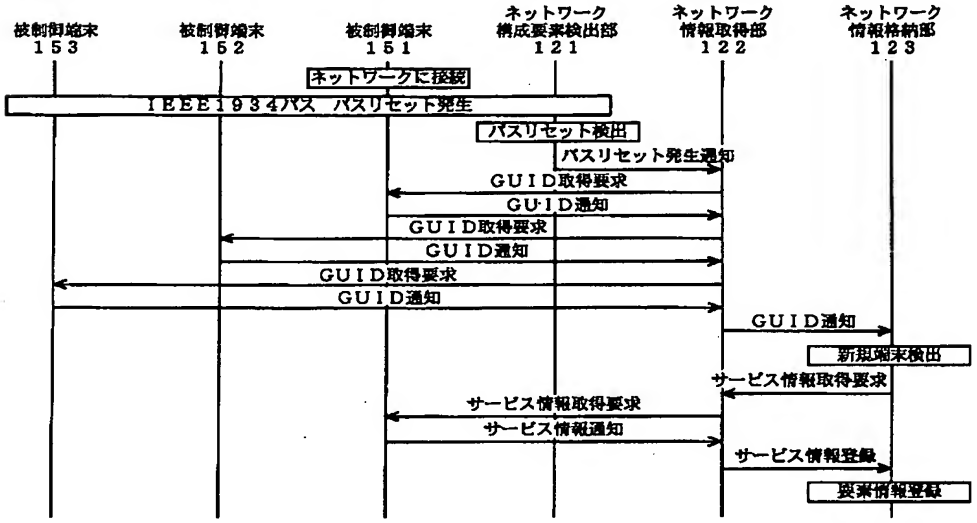
【図２１】

	GUID	ユーザID	制御端末のネットワーク	被制御端末のネットワーク	制限情報
新項目A→	0x0123456789012345	太郎	インターネット	IEEE1394	アクセス許可（1）
新項目B→	0x0123456789012345	花子	インターネット	IEEE1394	アクセス不可（0）
	0x0123456789023456	太郎	インターネット	IEEE1394	アクセス許可（1）
	0x0123456789023456	太郎	IEEE1394	IEEE1394	アクセス許可（1）
	0x0123456789023456	花子	インターネット	IEEE1394	アクセス不可（0）
	0x0123456789023456	花子	IEEE1394	IEEE1394	アクセス許可（1）
	0x0123456789034567	太郎	インターネット	IEEE1394	アクセス許可（1）
	0x0123456789034567	太郎	IEEE1394	IEEE1394	アクセス許可（1）
	0x0123456789034567	花子	インターネット	IEEE1394	アクセス不可（0）
	0x0123456789034567	花子	IEEE1394	IEEE1394	アクセス許可（1）

【図１７】



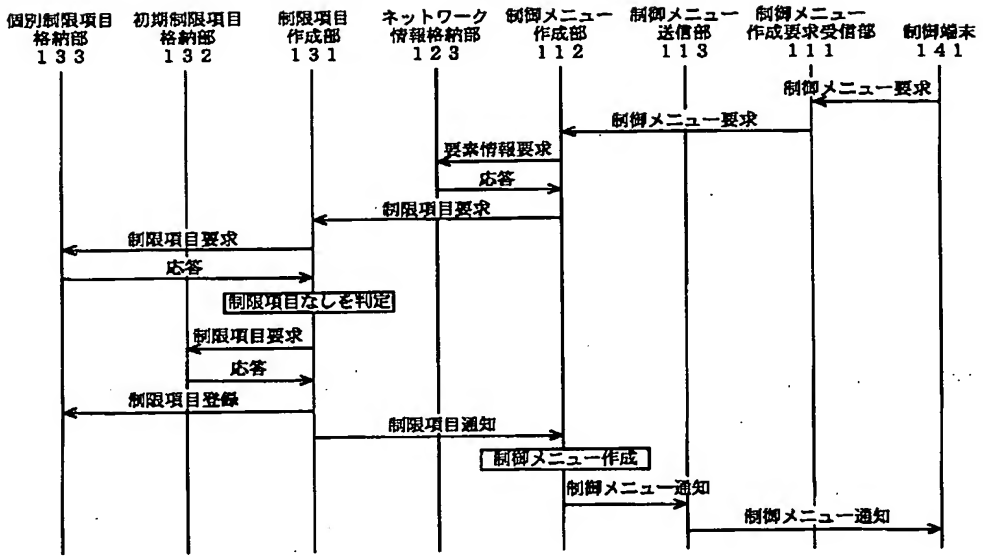
【図１９】



【図２２】

GUID	ユーザID	制御端末のネットワーク	被制御端末のネットワーク	制限情報
0x0123456789023456	太郎	インターネット	IEEE1394	アクセス許可（1）
0x0123456789023456	太郎	IEEE1394	IEEE1394	アクセス許可（1）
0x0123456789023456	花子	インターネット	IEEE1394	アクセス不可（0）
0x0123456789023456	花子	IEEE1394	IEEE1394	アクセス許可（1）
0x0123456789034567	太郎	インターネット	IEEE1394	アクセス許可（1）
0x0123456789034567	太郎	IEEE1394	IEEE1394	アクセス許可（1）
0x0123456789034567	花子	インターネット	IEEE1394	アクセス不可（0）
0x0123456789034567	花子	IEEE1394	IEEE1394	アクセス許可（1）

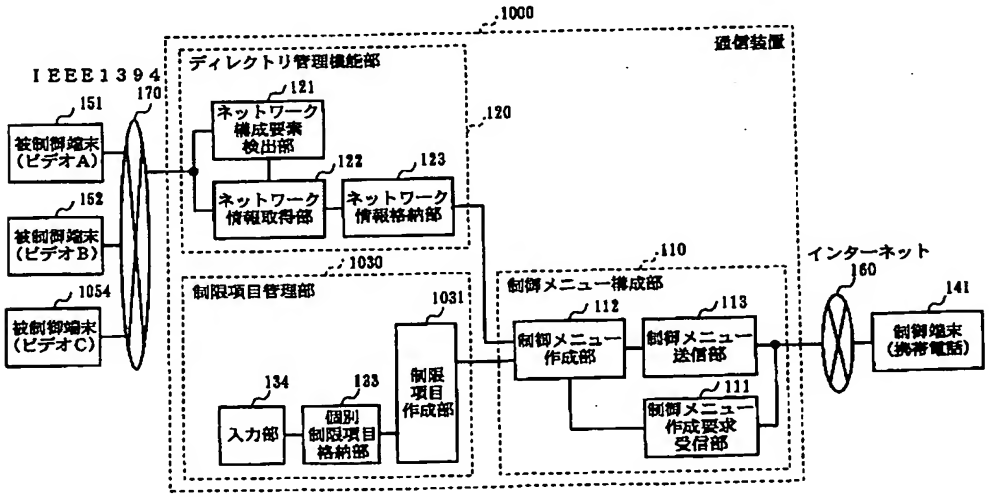
【図２３】



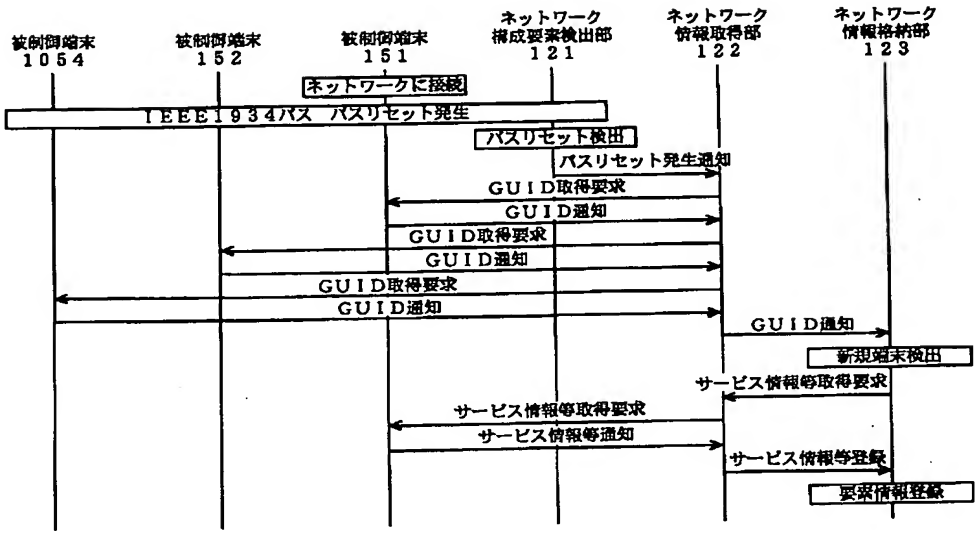
【図２４】

ユーザＩＤ	制御端末のネットワーク	被制御端末のネットワーク	制限情報
太郎	インターネット	ＩＥＥＥ１３９４	アクセス許可（１）
太郎	インターネット	ＯＴＨＥＲ	アクセス不可（０）
太郎	ＩＥＥＥ１３９４	ＩＥＥＥ１３９４	アクセス許可（１）
太郎	ＩＥＥＥ１３９４	ＯＴＨＥＲ	アクセス不可（０）
太郎	ＯＴＨＥＲ	ＯＴＨＥＲ	アクセス不可（０）
花子	インターネット	ＩＥＥＥ１３９４	アクセス不可（０）
花子	インターネット	ＯＴＨＥＲ	アクセス不可（０）
花子	ＩＥＥＥ１３９４	ＩＥＥＥ１３９４	アクセス許可（１）
花子	ＩＥＥＥ１３９４	ＯＴＨＥＲ	アクセス不可（０）
花子	ＯＴＨＥＲ	ＯＴＨＥＲ	アクセス不可（０）
ＯＴＨＥＲ	ＯＴＨＥＲ	ＯＴＨＥＲ	アクセス不可（０）

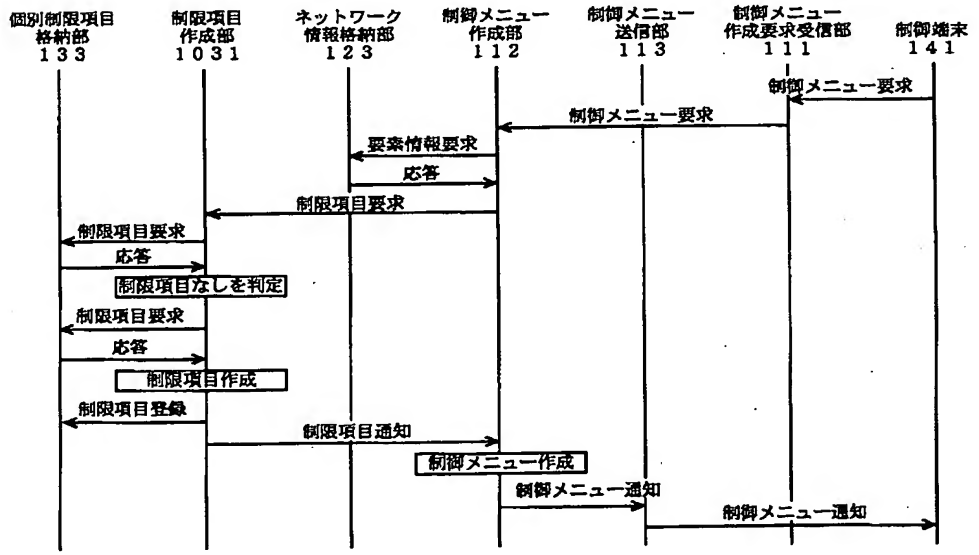
【図２７】



【図２８】



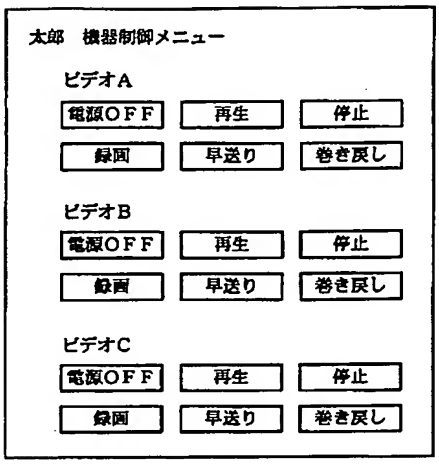
【図３０】



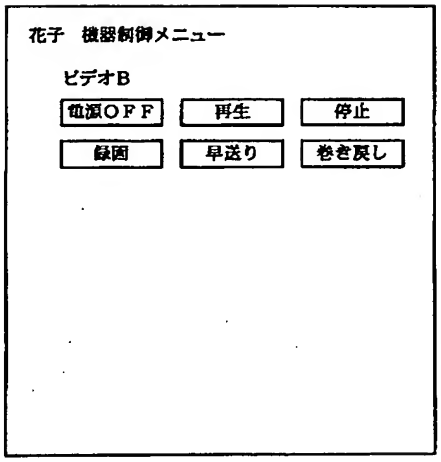
【図３１】

	ＧＵＩＤ	ユーザＩＤ	制御端末のネットワーク	機器カテゴリー	制限情報
新項目Ａ→	0x0123456789012345	太郎	インターネット	ビデオ	アクセス許可（1）
新項目Ｂ→	0x0123456789012345	花子	インターネット	ビデオ	アクセス不可（0）
	0x0123456789023456	太郎	インターネット	ビデオ	アクセス許可（1）
	0x0123456789023456	太郎	１ＥＥＥ１３９４	ビデオ	アクセス許可（1）
	0x0123456789023456	花子	インターネット	ビデオ	アクセス不可（0）
	0x0123456789023456	花子	１ＥＥＥ１３９４	ビデオ	アクセス許可（1）
	0x0123456789034567	太郎	インターネット	ビデオ	アクセス許可（1）
	0x0123456789034567	太郎	１ＥＥＥ１３９４	ビデオ	アクセス許可（1）
	0x0123456789034567	花子	インターネット	ビデオ	アクセス不可（0）
	0x0123456789034567	花子	１ＥＥＥ１３９４	ビデオ	アクセス許可（1）

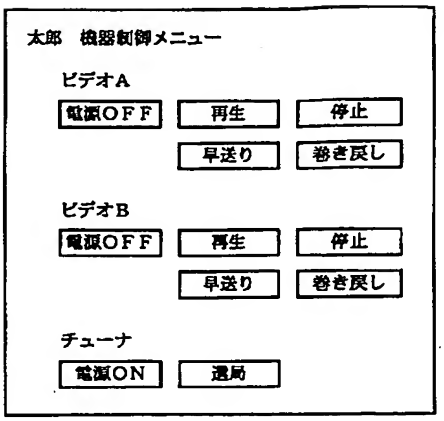
【図３３】



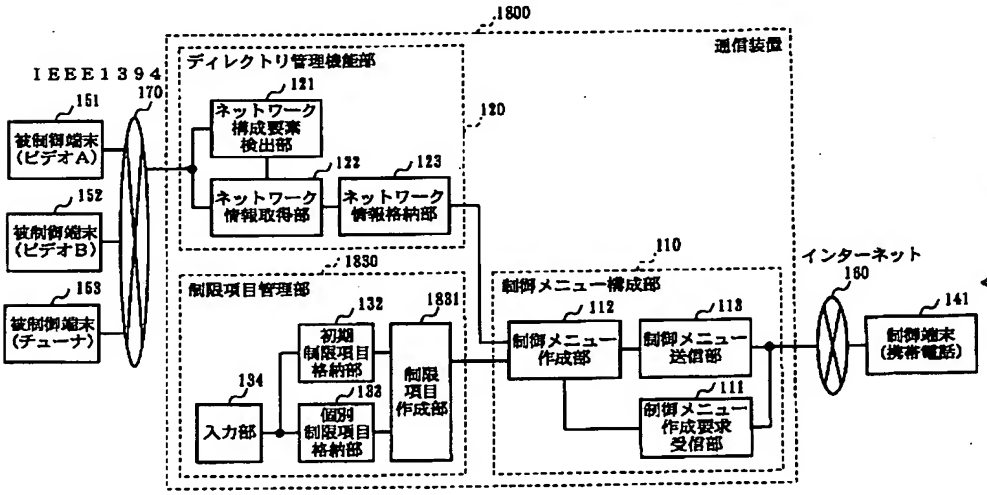
【図３４】



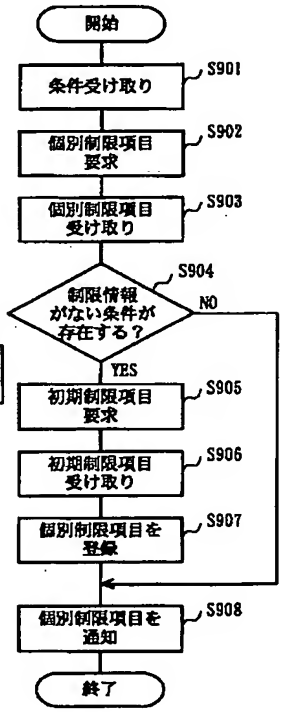
【図４３】



【図３５】



【図５０】



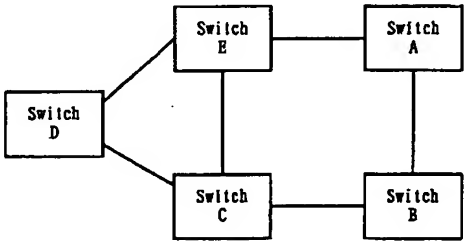
【図３７】

GUID	機器カテゴリー	サービス情報
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789034567	チューナ	電源、選局

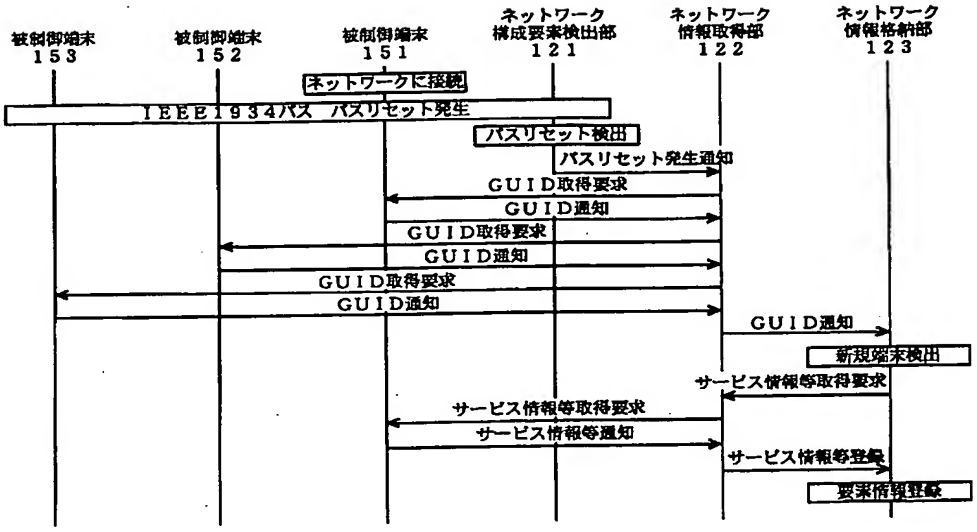
【図４６】

機器識別子	機器名	機器カテゴリー	サービス名	制御コマンド
0x0001	太郎のＰＣ	ＰＣ	ファイル送信	Ｆｉｌｅ
0x0002	花子のチューナ	ＡＶ機器	電源	POWER
0x0002	花子のチューナ	ＡＶ機器	選局	TUNE
0x0003	１階のエアコン	空調機器	電源	POWER
0x0003	１階のエアコン	空調機器	冷房	COOL
0x0003	１階のエアコン	空調機器	暖房	HEAT

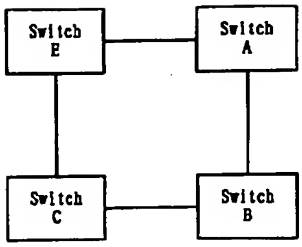
【図５２】



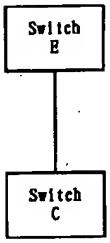
【図３６】



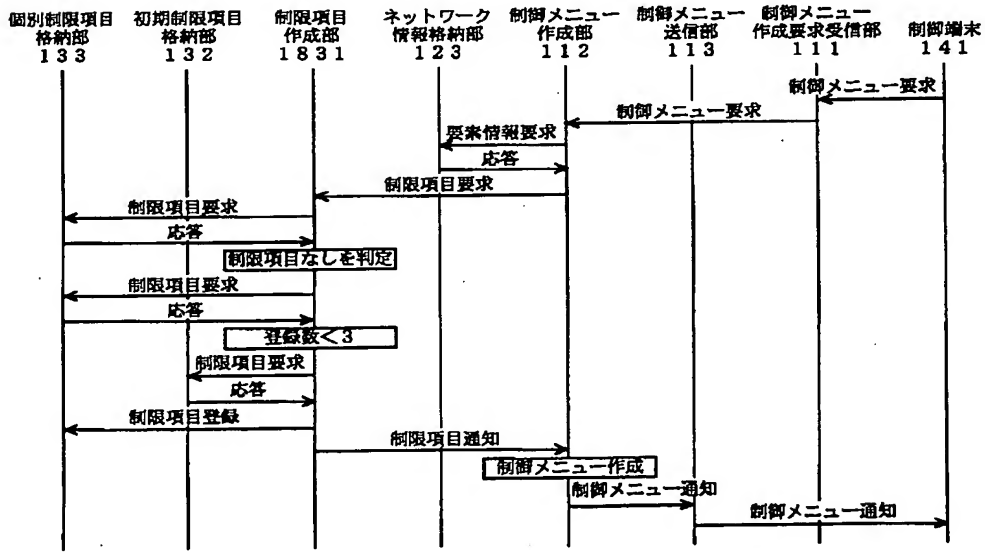
【図５３】



【図５４】



【図３８】



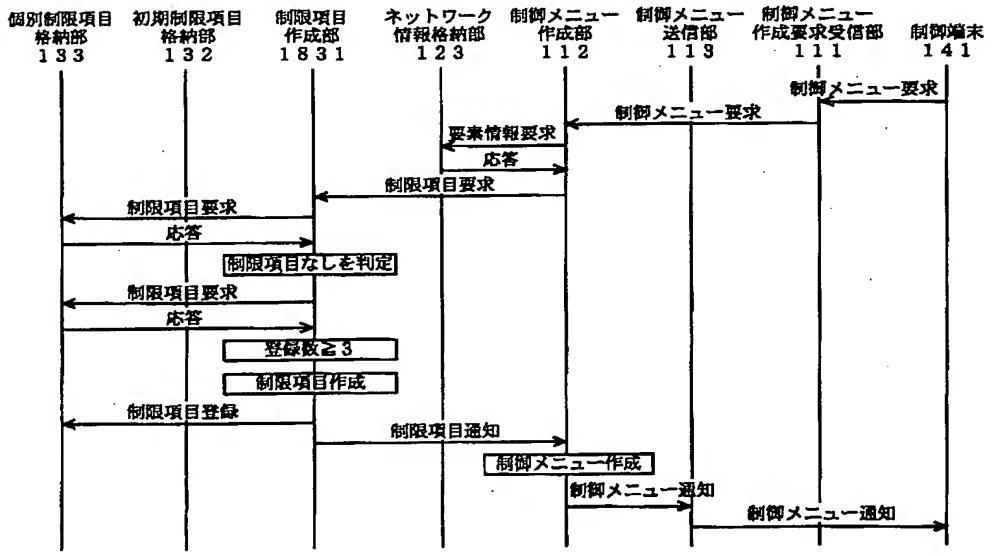
【図４０】

ユーザＩＤ	制御端末のネットワーク	サービス情報	制限情報
太郎	インターネット	電源	アクセス許可（１）
太郎	インターネット	録画	アクセス不可（０）
太郎	インターネット	再生	アクセス許可（１）
太郎	インターネット	早送り	アクセス許可（１）
太郎	インターネット	巻き戻し	アクセス許可（１）
太郎	インターネット	停止	アクセス許可（１）
太郎	インターネット	選局	アクセス許可（１）
太郎	インターネット	ＯＴＨＥＲ	アクセス不可（０）
太郎	ＩＥＥＥ１３９４	ＯＴＨＥＲ	アクセス許可（１）
ＯＴＨＥＲ	ＯＴＨＥＲ	ＯＴＨＥＲ	アクセス不可（０）

【図３９】

	GUID	ユーザID	制御端末のネットワーク	サービス情報	制限情報
新項目A →	0x0123456789012345	太郎	インターネット	電源	アクセス許可（1）
新項目B →	0x0123456789012345	太郎	インターネット	録画	アクセス不可（0）
新項目C →	0x0123456789012345	太郎	インターネット	再生	アクセス許可（1）
新項目D →	0x0123456789012345	太郎	インターネット	早送り	アクセス許可（1）
新項目E →	0x0123456789012345	太郎	インターネット	巻き戻し	アクセス許可（1）
新項目F →	0x0123456789012345	太郎	インターネット	停止	アクセス許可（1）
	0x0123456789023456	太郎	インターネット	電源	アクセス許可（1）
	0x0123456789023456	太郎	インターネット	録画	アクセス不可（0）
	0x0123456789023456	太郎	インターネット	再生	アクセス許可（1）
	0x0123456789023456	太郎	インターネット	早送り	アクセス許可（1）
	0x0123456789023456	太郎	インターネット	巻き戻し	アクセス許可（1）
	0x0123456789023456	太郎	インターネット	停止	アクセス許可（1）
	0x0123456789023456	太郎	IEEE1394	OTHER	アクセス許可（1）
	0x0123456789034567	太郎	インターネット	電源	アクセス許可（1）
	0x0123456789034567	太郎	インターネット	選局	アクセス許可（1）
	0x0123456789034567	太郎	IEEE1394	OTHER	アクセス許可（1）

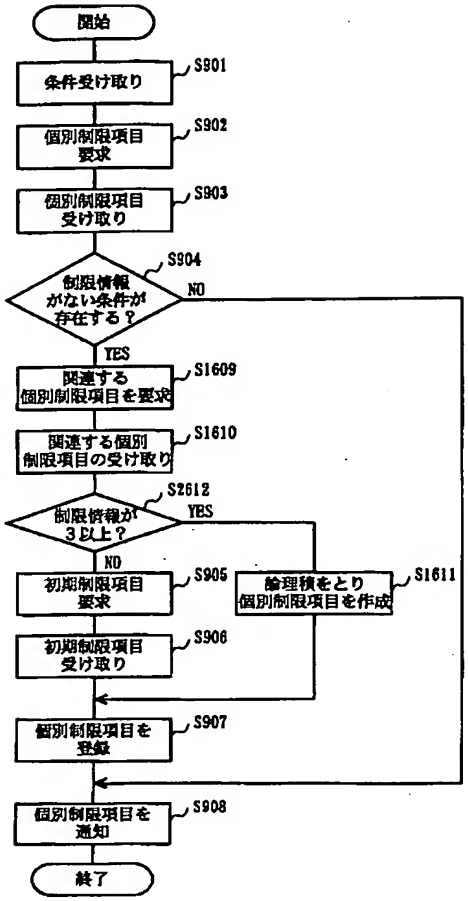
【図４１】



【図４８】

	機器識別子	制御端末のネットワーク	被制御端末のネットワーク	制限情報
	0x0001	宅外	宅内	アクセス不可（0）
	0x0001	宅内	宅内	アクセス許可（1）
	0x0002	宅外	宅内	アクセス許可（1）
	0x0002	宅外	宅内	アクセス許可（1）
新項目A →	0x0003	宅外	宅内	アクセス許可（1）

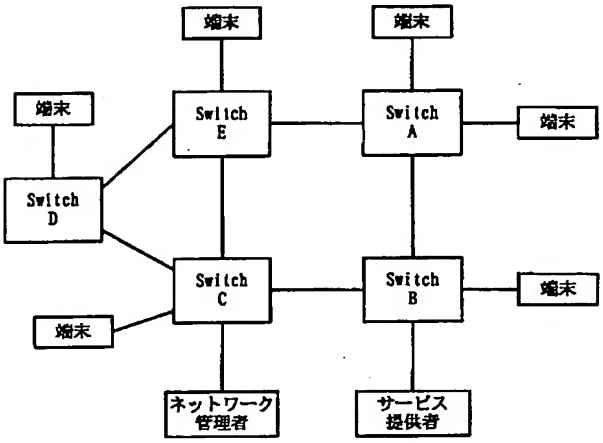
【図４２】



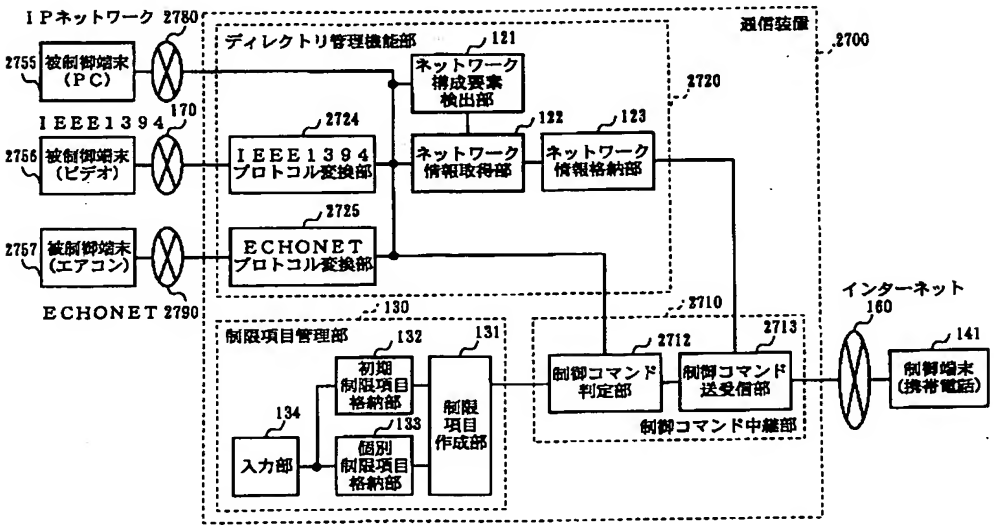
【図４９】

制御端末のネットワーク	被制御端末のネットワーク	機器カテゴリー	制限情報
宅外	宅内	ＰＣ	アクセス不可（0）
宅外	宅内	ＡＶ機器	アクセス許可（1）
宅外	宅内	空調機器	アクセス許可（1）
宅内	宅内	ＰＣ	アクセス許可（1）
宅内	宅内	ＡＶ機器	アクセス許可（1）
宅内	宅内	空調機器	アクセス許可（1）

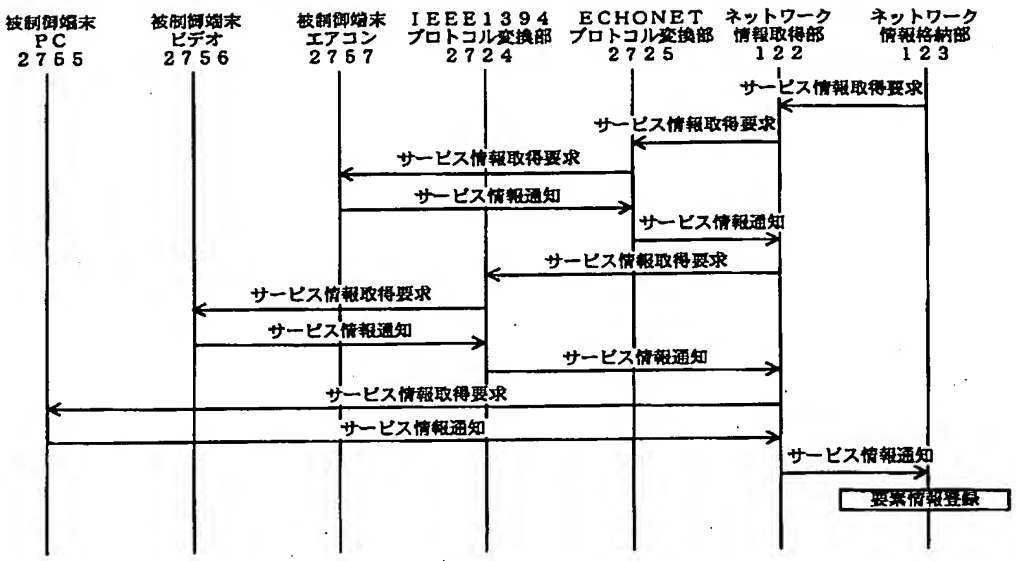
【図５１】



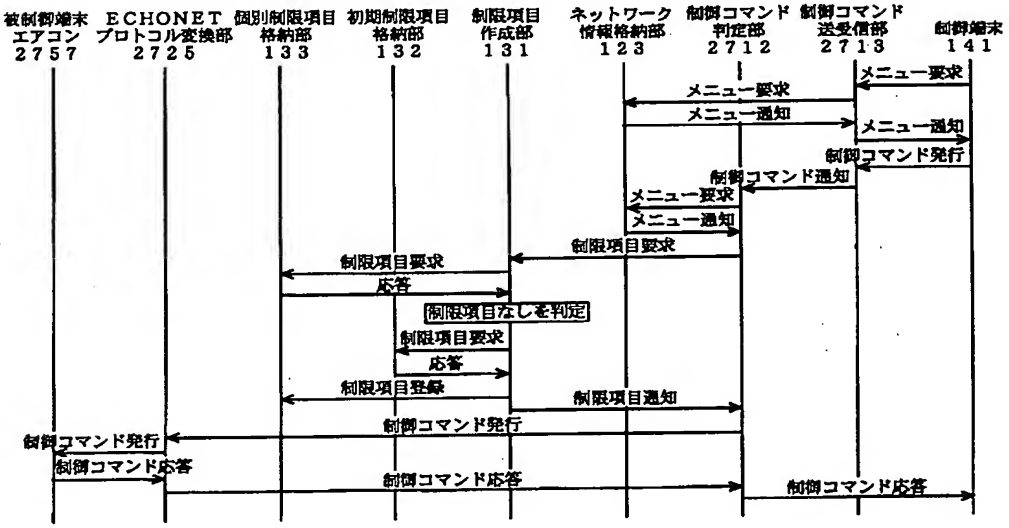
【図４４】



【図４５】



【図４７】



フロントページの続き

(72)発明者　久保田　幸司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　斉藤　孝弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　石川　博一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B085 AE00 AE02 BC02
5B089 KA17 KB13
5K030 GA15 HD03 HD06 HD09 LD20
5K033 AA08 CB09 DA06 DB18